Master Thesis, 20 credits.
Master of Law Program.
Department of Law,
School of Economics and Commercial Law.
Göteborg University, March 2005.

A Legal Analysis of Cheating in Online Multiplayer Games

Author: Joel Zetterström

Supervisor: Kristoffer Schollin

Examiner: Ulf Petrusson

Center for Intellectual Property Studies

School of Economics and Commercial Law
GÖTEBORG UNIVERSITY

”Just how seriously should you as a developer take the possibility of online cheating? If your game is single-player only, then you have nothing to worry about. But if your game is multiplayer only, the success of your entire product is at stake… Cheating undermines success.”

- Matt Pritchard, Game Software Developer.[1]

“Cheating is the bane of online gaming: be paranoid”

- Shawn Hargreaves, Game Software Developer.[2]

“We as well as everyone else gains on having a cheat free product.”

- Lars Gustavsson, Lead Designer at DICE.[3]

“There are a handful of people out there that get a rise from destroying other people's play experience. You can't get rid of it totally. We just try to address it as it comes up.”

- Minh “Gooseman” Le, Creator of Counter Strike.[4]

If you wish to contact the author, send an email to; joelzetterstrom@hotmail.com

[1] Pritchard, http://www.gamasutra.com/features/20000724/pritchard_pfv.htm
[2] Hargreaves, http://www.talula.demon.co.uk/ConsoleOnline.pdf
[3] DICE made Battlefield 1942, the quote was regarding their upcoming FPS Battlefield 2. Reinius, http://www.bfcentral.se/?s=article_show&id=525&pn=9
[4] Rolston, P 4. http://www.avault.com/articles/getarticle.asp?name=gooseman&page=4

Abstract

This Master Thesis deals with the legal issues of cheating in online multiplayer games, particularly in the three major game genres; First Person Shooters, Real Time Strategy and Massive Multiplayer Online Role-playing games. The industry is growing rapidly as Internet connectivity increases, and is thus forced to face new challenges; specifically the problem of cheating in online games. This paper examines and analyses legal strategies that can be used to combat cheating, ending with conclusions on how and when they can be used most effectively to limit the amount of cheats in computer games.

Because of the global nature of the Internet and the gaming industry, the legal focus is placed on the United States and the European Union. Law differs from country to country, but international conventions provide a common ground – especially regarding Intellectual Property rights. The European Union have produced a number Regulations and Directives that the member countries are obligated to uphold nationally, thereby creating a somewhat harmonized legislation that can be used to make legal predictions valid for all member states. This is augmented with a US perspective, which probably is the single biggest market for computer games.

The first part of the thesis describes the phenomenon of online gaming in order to provide a sufficient background on the subject for the uninitiated reader, but also to examine the mechanisms of, and structures behind, cheating. The second part examines the processes of how cheats are created and the legal measurements that can be used to prevent such creations, specifically copyright laws. The third part focuses on the spreading of cheats, if and how such spreading can be stopped with legal means. Trademark laws together with rules about the takedowns of websites containing illegal material are analyzed and discussed. The fourth part deals with the use of cheats in the games, and how such use can be stopped with contractual means. The validity of wrap agreements, i.e. electronic contracts, with specific examples is examined and their effectiveness evaluated. Part five of the thesis contains a brief examination about cheating as a crime, and criminal law pertinent to the subject is provided. The sixth part compares the phenomenon of cheating in cyber sports to that of regular sports, and if lessons learned in the sports world about cheating (specifically doping) can be carried over to cyber sports. The thesis ends in a conclusion part which discusses the findings of the above mentioned chapters in an effort to find the most effective legal strategies that can be used to limit cheating in online computer games.

Table of Contents

Chapter 1: Preface

1.1 Foreword

Playing computer games online has been, and is, a favourite pastime of mine, just as many other young men and women[5] of my generation. And just as everyone else, I soon encountered the issue of cheating, and how cheats can ruin an otherwise good game. I witnessed how the gaming companies tried to limit the problem with evermore advanced software. Sometime during my studies for the Master of Law, an idea struck me; what legal strategies can be used to combat cheating? The software approach was clearly, in my estimation, not sufficient to alone halt cheating. Combining the two approaches ought to lead to much better results.

It is my hope that gaming companies, like developers and publishers, can read this essay and get inspiration and ideas on how to use the law in order to combat cheating. I also wrote this essay with the intention that gamers interested in the subject could get a clear overview on the legal aspects of cheating. I do not how many misguided forum threads I have read on the subject, so I hope that this can bring some clarity to the debate. Finally, I hope that practitioners of the law that come across this subject in their work could refer to the essay as a source for help and guidance.

Joel Zetterström
Gothenburg, March 2005.

[5] When I hereafter write “he”, it could just as well refer to a “she”. It is for reasons of simplicity only that I write he, him etc.

1.2 Scope of the Essay

The intention I had in mind when I wrote this paper was to answer the question; *how can and should the law most effectively be used to combat cheating in online multiplayer games?* I further narrowed down the problem to deal only with those cheats that are called "hacks" and "bug-exploit", the two most common ways of cheating – see Chapter 2.4 for a taxonomy of cheats in online computer games. To answer this question, I partitioned the problem in four areas and analyzed corresponding laws;

1. The creation of cheats	Copyright law
2. The spreading of cheats	Trademark and "takedown" laws
3. The use of cheats	Contract law
4. Cyber crime	Criminal law

I also did a comparison between sports and cyber sports, to see if there was anything that can be learned from the sports worlds struggle against doping and applied to cyber sports.

1.3 Method and Material

The usual method of writing a Master Thesis of Law is fairly straightforward. A problem is formulated, followed by an information gathering process. Thereafter the prominent authors on the subject are referred to, and a subsequent conclusion is drawn, intermingled with the authors own opinion. This essay had to deviate from this formulae for one simple reason; not many (I have not seen a single one) authors have dealt with the issue of legal aspects of cheating in online multiplayer games. Therefore I was frequently forced to draw my own conclusions from studies of the law, existing doctrine and other relevant sources, and apply them to the situation at hand, instead of relying on authorities on the subject and merely referring their opinions.

The material used also differs from the 'normal' thesis. Much of it is fairly new, and many of the issues described have yet to make their way into the traditional Medias of law; books and printed articles in legal magazines. The Internet however, houses an abundant wealth of material pertinent to the subject. The international aspect of the paper also benefited from the relative ease which articles from all over Europe and United States can be found on the web. Every link used as a reference was visited by me during

the first quarter of 2005, which of course is not a guarantee that they will be up for any length of time. Nevertheless, articles are frequently only relocated and a search on the exact article name is often profitable if a specific link fails.

The global aspects of online gaming meant that an analysis valid for only one country, say Sweden, would be fairly useless. I have therefore tried to be as international as possible, using international conventions and treatises as sources of law whenever applicable, as many of them referred to in this paper are signed by a large number of countries worldwide. It should be noted though, that the implementation of such conventions can differ from country to country. I have further focused the legal analysis on two major areas, the United States (US) and the European Union (EU), and something should be said about the legal situation in Europe. The EU member countries are obliged to obey the rules of the Union, naturally, and the EU legislates, among other things, via Regulations and Directives. However, only Regulations and certain Directives are directly valid as law in the member states. Most Directives require implementation, i.e. rewriting national laws to match the Directive. Such implementation can take years, and different countries may choose to implement Directives in slightly different ways. Nevertheless, basing the European analysis on Regulations and Directives should mean that the conclusions are basically valid for the entire Union.

Chapter 2: Introduction

The computer industry is growing, rapidly. Computers, rare only twenty years ago, are now in every office and almost in every home. A whole generation of kids have been brought up, and are being brought up, playing electronic games. A multibillion dollar industry has emerged; one geared towards providing games in various shapes and forms, and with the new industry comes new ways of making business. The Entertainment Software Association (ESA) reported that US sales of computer and video games reached over seven billion dollars in 2004[6], and the world market was estimated to 18.5 billion dollars in 2003[7] by the Entertainment and Leisure Software Publishers Association (ELSPA). Other figures are significantly higher; wired.com reported 30 billion dollars in global sales for 2002.[8] The growth is estimated to something like 20 % a year, which makes it one of the fastest growing industries today.

The Internet usage has exploded; broadband connections are replacing the old modems, and with broadband access to the Internet come new business opportunities. Online multiplayer gaming is a growing genre, and some games are directly targeted for online play. The online environment brings new challenges with it, new ways of distributing games and new ways of extracting money from customers. A few years back, the multiplayer part of a game was almost incidental rather than deliberately planned to entice customers. Now we see games directly targeting the multiplayer aspect. Consider Counter Strike (CS), allegedly the worlds most popular game[9], which was a game created for multiplayer exclusively, or the game Battlefield 1942 – a game that though it came with a single player mode was intended for multiplayer almost exclusively. Not to forget is the popular genre called Massively Multiplayer Online Role Playing Game, or MMORPG, whose very purpose is to create worlds in which people can play online. The console market is also catching up. The major consoles, Xbox, GameCube and Playstation 2 all have online multiplayer game opportunities. Although predicting the future is never easy, all factors seems to indicate that online gaming will grow, and will contribute significantly to the growth of the industry[10]. As high-speed Internet access continues to be available to more and more people, more people will begin playing games online.

---

[6] http://www.theesa.com/archives/2005/02/computer_and_vi.php
[7] http://www.elspa.com/about/pr/pr.asp?mode=view&t=1&id=368
[8] Gaudiosi, http://www.wired.com/news/games/0,2101,61358,00.html.
[9] Counter Strike was a "modification" originally, but more on mods later, in Chapter 3.3.
[10] Kofler et. al. P 25. http://ep2010.salzburgresearch.at/knowledge_base/kpmg_2002.pdf

The major challenge the industry has had to face as of yet is probably piracy. Some people "crack" the games and release them on the Internet, thus allowing those who have not bought the game to download it and play it. If the cracked game is used to play singleplayer only, i.e. not requiring access to the Internet, these cracks are virtually unstoppable. However, a multiplayer game session requires an Internet connection, and gives the ability to check that the player's copy of the game is legitimate. Thus a good multiplayer in a game may mean that some people will buy the game legitimately only to be able to play online.[11] The idea is to provide value beyond a copy of the game, e.g. in multiplayer, added features, continuous support etc.[12] This also means that companies are able to devise new ways of value extraction. For example most MMORPG's require some sort of regular subscription fee, in addition to buying the game itself, for playing the game online (MMORPG's are only playable in online mode).

But this online architecture has brought with it new problems, particularly the phenomenon of cheating.

2.1 Why Cheating is a problem

"It is only a game, who cares?"

I received this question numerous times when I explained the content of this paper to fellow law students, teachers, friends and other uninitiated. (However, those who play or had played games online had generally no problem in immediately recognizing the problem.) They seem to think of online gaming as something akin to a round of monopoly at the kitchen table. Sure, your buddy may have moved his piece a step to far when you were not looking, or even sneaked a few dollars from the bank. Maybe you caught him and you both had a good laugh. After all, it is only a game, right? Let me tell you a little story then, about a chess player, before the Internet age. He is quite good at chess, and engages everyone around him as much as he can. But since he always wins, both he and his friends in the local chess club tire of playing him. He loves playing chess though, so he searched for other options. He can not go professional and travel around the country or the world playing, he has his family and career to think about, and he is not

[11] This is not always true. In some games it is possible to create cracked servers, meaning that people with cracked copies of the game can play online on these servers.
[12] Wardell, P 3. http://www.avault.com/developer/getarticle.asp?name=bwardell3&page=3

quite good enough to match the best anyway. One day he sees an ad in the newspaper for a correspondence chess league, and joins up with a heart soaring with joy. The players schedule evening matches and phones, fax or mail their moves to each other. Our chess player takes to it like a fish in the sea, and for a time he is happy. The third season he participates he even figures he has a chance of winning- but then the unthinkable happens. A guy, consistently low placed, and who he has beaten every time up until now totally wipes the table with him and the guy precedes to win every game becoming uncontested season winner. The community is outraged, how could he have become so much better in just a few months? Eventually the guy who won confesses, he had bought one of the new chess boards with an onboard computer that played for him. He cheated. Our friend totally loses his spirits; the correspondence chess league is now swamped with players who use chess computers to defeat tough opponents. The paranoia hits the community; almost every good player is now accused of cheating. Where once good mood with many a call of "good job, nice match!" reigned, now all one hear is "you cheated, you bastard!" Disgusted he leaves the league never to return…

Now, replace the correspondence chess league with any online FPS or RTS-game. Or imagine you spending countless of hours building up a powerful character in an MMORPG with level 40, and encountering an entirely new player with level 80 asking you what a "quest" is, who then proceed by killing your character with the rarest sword in the game available only to the best.

The facts are that cheating is a major concern for online gamers; a study showed that 66 % of the participants complained about there being too many cheaters[13]. And when it is a problem for the players it becomes a problem for the developers and the publishers. It is all in the brand. If a game gets a reputation for containing too many cheaters, players will leave the game. In all likelihood, they will not buy expansion packs, they will certainly not pay subscription fees and it is doubtful if they will return to the next instalment of the game. The brand will lose value, and the companies behind the game will lose money. With the growth of the gaming industry and the proliferation of online gaming, it is only matter of time before the problem of cheating in online multiplayer games will receive mainstream attention proportional to the size of the industry. New

13 Egenfeldt-Nielsen et. al. http://www.game-research.com/art_online_gaming.asp.

York Times published an article in 2003 that recognized the problem;[14] QuakeWorld, a popular game in the mid 90´s, had a huge community. Then cheats were released and the community went from teeming with players to a wasteland. This is not something you want to happen to your game.

2.2 Background – Online Multiplayer Gaming

In order to understand what cheating is, one must have some inclination as to how online gaming is functioning. The reader already acquainted with the online gaming scene should probably skip chapter's 2.2 and 2.3.

There are three major genres in online multiplayer gaming, namely First Person Shooters (FPS), Real Time Strategy games (RTS) and Massively Multiplayer Online Games (MMOG). There are certainly other game types played online, but these three genres contain a vast majority of the online gamers. Another type of genre is also growing rapidly online, that of games of chance, e.g. poker, black jack and other such casino games, but these types of games are not subjected to cheating in the same way. See Chapter 6 for further details. Simple online games, like small browser-based games, are not within the scope of this paper as cheating in those game-types are non-existent even though some of them are available in multiplayer mode.

The reader unfamiliar with these terms (FPS and RTS) can read these excellent articles for detailed explanations of the genres: http://en.wikipedia.org/wiki/First_person_shooter and http://en.wikipedia.org/wiki/Real-time_strategy

The genre of MMOG differs in significant ways from the two other major online genres. An MMOG creates a persistent world which can, at any given time, house thousands and thousands of players on the same server. See http://en.wikipedia.org/wiki/Massively_multiplayer_online_game and http://en.wikipedia.org/wiki/MMORPG (Massively Multiplayer Online Role-playing Game, the biggest subgenre of MMOG's) for more information. The goal for most players is to have the highest level and the most powerful objects and possessions.

[14] Wayner, http://tech2.nytimes.com/mem/technology/techreview.html?res=9B0DE6DC1E30F934A15750C0A9659C8B63

Creating powerful characters and gaining powerful possessions takes a lot of time, and some players spend a huge amount of time online in the world to achieve the goal of a mighty avatar. This has spawned an artificial economy, where objects in the game have a value in the real world, besides their value within the MMORPGs economy. Items and powerful characters (the character, or avatar, is linked to an account, which can be transferred to other people, or in some cases someone can transfer the character itself to another account) from MMORPGs are sold regularly at eBay or special sites for this purpose, like PlayerAuctions[15]. A company, Black Snow Interactive from southern California, even hired three shifts of underpaid Mexicans and had those playing popular MMORPGs. The accounts and objects the Mexicans gained where then sold, which elicited a heated debate when Mythic Entertainment (owner of one of the games in question) sued them for intellectual property infringement.[16]

2.3 Online and offline play, clans, and the professional scene

Both FPS and RTS-games can usually be played in singleplayer mode, as opposed to multiplayer (called sp and mp respectively). Sp does not require Internet access, and the player steers his character trying to defeat the computer rather than characters controlled by other humans. Before the Internet virtually all games were played in singleplayer, in fact before Internet access became as widespread as it is today singleplayer was the only option for most people. Cheating in singleplayer is not a problem, as you only play against a computer, not other humans. In fact, most developers release sp-cheat codes to the players that can not be used in mp (unless the developers screw up). It is a possibility that the existence of sp-cheats makes the cheat creation process easier, as cheat-creators can study the sp-cheats and learn how to incorporate them into an mp-cheat. (When I talk about cheats and hacks in this paper, I generally mean mp-cheats.) It is possible to compete in computer games, by playing matches. This can be done one on one, which is most common in RTS, but also a team versus another team, which is most common in FPS. These teams are called clans, and they compete against each other on *ladders*, leagues, in tournaments and cups, organized by what I choose to call a ladder-organization. Matches that are not clan against clan are played just for fun, and are thus called “fun-games”. MMOG’s are not played competitively in the same way, but people can choose to cooperate in the MMOG equivalents of clans, called guilds.

[15] http://www.playerauctions.com/ eBay is found at http://www.ebay.com/.
[16] Dibbel, http://www.juliandibbell.com/texts/blacksnow.html

An alternative to Internet is something called LAN[17], which allows mp against the other people connected to the LAN. MMOG's does not have a sp-mode, and are not playable on LANs.

The widespread popularity of some games has spawned a professional scene. The best clans and individuals in the world actually get paid to play the game fulltime, if the game is big and can attract sufficient amounts of interest, and these professional players are financed via prizes in tournaments and cups, and sponsorships from the gaming related industry. The biggest professional tournament organization is Cyberathlete Professional League[18], which regularly organizes tournaments around the world. All professional competitions are played in a LAN, in part to eliminate latency issues[19], but mostly because cheating is extremely difficult when playing on LANs. Since a bystander can simply stand behind and look at the players screen, cheating will be spotted immediately on LANs. Currently the only absolute, foolproof way of making sure some does not cheat is to spectate that person playing, i.e. standing behind him and looking at his screen.

2.4 Cheats in Online Computer Games

A taxonomy of cheats was suggested by Yan and Choi in the paper called "Security issues in online games"[20], which indicates eleven specific areas of cheats. They defined cheating as; *"Any behaviour that a player may use to get an unfair advantage, or achieve a target that he is not supposed to is cheating."* As I will explain below (Chapter 2.4.2), defining cheats is not as simple as that.

1. Cheating by collusion. This can occur in games where one player is not suppose to know what other players know but exchanges information anyway, such cheat can for example occur in an online version of the card game Bridge. In FPS and RTS, players are allowed and encouraged to cooperate if they play on the same team, and it is very common to do that by using voice chat programs.

[17] LAN, Local Area Network, is two or more computers connected to each other directly, i.e. not via the Internet, although the LAN itself can be connected to the Internet.
[18] http://www.thecpl.com/
[19] Playing over the Internet requires communication, e.g. between server and client. When the communication is slow the result is high latency, dubbed "lag" in Internet slang. Lag slows down players reactions, as people without lag will be able to have their actions recorded by the server faster.
[20] Yan et. al.
http://ariel.emeraldinsight.com/vl=2848761/cl=20/fm=html/nw=1/rpsv/cw/mcb/02640473/v20n2/s6/p125

2. Cheating by abusing procedure or policy. Some games record wins and losses for each player profile in a statistic database[21] and by abusing certain procedures the player can escape having his loss recorded. The winner will therefore not have his win recorded.
3. Cheating related to virtual assets. The trading of virtual assets is a big business worth lots of real money, and thus cheating related to virtual assets is attractive. Trading in MMORPG's can therefore be abused by certain players who accept the money for an item, but then keep it.
4. Cheating by compromising passwords. Passwords (I would say that this category also includes CD-keys) for online games can be vulnerable targets for malicious users. Once acquired, they can be used access crucial game data and authorization thus enabling cheats in various ways, for example to steal items from another player or to block his access to the game (see number 5 below).
5. Cheating by denying service to peer players. Various techniques, like flooding the other players connection so he times out, or forcing him to disconnect (disconnect hack) at the right time can lead to benefits in computer games.
6. Cheating due to lack of secrecy. Servers and computer communicate with each other with packets of information. These packets can be intercepted and read, or inserted with different data, enabling cheats.
7. Cheating due to lack of authentication. This is cheats related to authentication between server and client.
8. Cheating related to internal misuse. Game operators and system administrators have special power over a gaming environment that could be misused in order to cheat, an example can be to create valuable items in MMORPG's and sell them.
9. Cheating by social engineering. There are various ways of scamming people to get access to their passwords and CD-keys, e.g. by posing as a system administrator.
10. Cheating by modifying game software or data. This is the traditional way of cheating in online multiplayer games. Cheat-creators can reverse engineer the gaming software and create special programs that can be used to gain unfair advantages. This is also called "hacks", and I delve deeper into this subject in Chapter 3.2.
11. Cheating by exploiting bug or design flaw. A very common way of cheating, described more extensively in Chapter 2.4.1 below.

This paper deals only with legal strategies on how to limit the most ubiquitous and therefore most damaging types of cheats, namely that of number 10 and to some extent

[21] Like http://www.battle.net/, where WarCraft and StarCraft are laddered.

number 11 of the taxonomy above. To describe, analyze and conclude legal strategies for all types of the cheating mentioned above would be the subject of a book, not a Master Thesis.

2.4.1 Exploiting Bugs

Something considered a cheat, but is not a hack, is the exploiting of "bugs" sometimes called "sploitz". A definition of bug is; *"A computer bug is an error, flaw, mistake, failure, or fault in a computer program that prevents it from working correctly or produces an incorrect result. Bugs arise from mistakes and errors, made by people, in either a program's source code or its design."*[22] It is generally so that every game comes with bugs, even if well coded games contain fewer bugs than badly coded. A synonym to bug in this context is *glitch,* and the bug exploiter is called *glitcher*.

Exploiting bugs can be done in many different ways, depending on the type of the game and the bug itself. For example, a common bug in some FPS-games allows players to reach areas of map that is not suppose to be accessible, and from these areas they are invisible to other players. Hence they can shoot other players undetected. Trying to list every bug that has been exploited is of course impossible; suffice it to say that there probably are bugs for every game ever released. Some are severe, some negligible and some are not even noticed by the majority of the players. Generally though, bugs are not that big of a problem compared to hacks, people exploiting bugs are often easy to spot. The problem arises when the glitcher exploits a bug not visible to other players. The exploiting is then tantamount to hacks, e.g. exploiting a bug that lets the player see through walls.

The existence of a certain bug in MMORPG's is so severe that it is worth mentioning individually. In some MMORPG's certain techniques allows the players to duplicate items, the action being called "duping". Duping is a form of bug exploitation, but it can also be a combination of hack and exploiting.

A game with good support from the developer and the publisher will have *patches* released. A patch is an update to the game that focuses on fixing bugs and other game play issues, but some also release new features in their patches.

[22] http://en.wikipedia.org/wiki/Computer_bug

2.4.2 Defining Cheats – The grey area

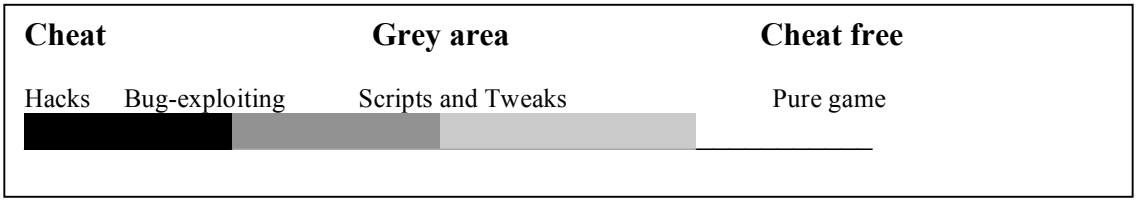
As any good legal practitioner knows, defining terms is perhaps the most important job for a lawyer. If two parties meet and agree to not "cheat", you can bet that they will end up fighting over what "not cheating" actually means. The common usage of the word cheat will of course provide some common ground for the two disputing parties; any dictionary will define cheat, in this context, along the lines of *deliberately violating rules in a game*. This does not provide us with much help, does it? What are the rules for a computer game? Is there some manual somewhere that details how the game is suppose to be played? The answer to those two questions are usually no, although most ladder organizations put up their own rules. Many MMORPG does also have a Code of Conduct which may include rules on what is considered to be cheating. It also generally agreed that anything a player does to get an *unfair* advantage is a cheat, but this just shifts the definition problem from *cheat* to *unfair*.

The fact that having a good computer connected to the Internet with a high speed broadband is not considered unfair or a cheat, although it is an advantage, has led most online PC gamers to engage in an activity called "tweaking", which means to alter various inputs on the computer and in the game to enhance performance and personalize settings. For example, the primary tweak objective in FPS-games is usually to achieve as many frames per second (fps[23]) as possible. A high value for fps means that the game will run smooth, and allows the player to react faster than a player with too low fps. Tweaks are also done to personalize the setup for a player, because different hardware needs different settings to work optimally, and because different people prefer different settings. The developer of a game therefore leaves a file open for editing for tweaking purposes, the file is usually called "configuration" (cfg). But developers make mistakes (as we saw just above in Chapter 2.4.1 about bugs), leaving certain settings open although they should perhaps be closed, and hence some tweaks may be considered cheats by the community. For instance, an option to turn off the fog in game can greatly reduce the workload on a graphic card and thus enhance performance. But on the other hand, a player without fog will see much farther than players with fog enabled – and the map which was suppose to be played with fog are disrupted in its game play when players can see across it. Therefore turning off fog is considered a cheat in most FPS-gaming

[23] Confusingly enough the abbreviation is exactly the same as First Person Shooter, the game type in which frames per second matters the most. To distinguish between the two, frames per second is written in small letters – fps, and First Person Shooter is written in capital letters – FPS. A good article explaining the phenomena of fps can be found here: http://amo.net/NT/02-21-01FPS.html.

communities. Another example is the option to turn off the ambient sounds. This may not be possible to do in the in-games menus, but with a little tweaking a player can make them disappear. This allows him to hear the footsteps of his opponents much clearer, and players with ambient sounds still on will be disadvantaged. To further complicate matters, some players, although they are few, define every tweak not done inside the game (all games have menus that allow the player some basic tweaks, like changing screen resolution) as a cheat. This, i.e. only playing with tweaks done in-game, is called playing the game "out-of-the-box".

Another tool that is available in some games is *scripting*, also called a *macro*.[24] A script is, in the gaming world, a line or several lines of script code that automates tasks the user might otherwise perform interactively on the keyboard. A commonly used variety of scripts in many games is the assignment of different actions to keyboards. Let us say that you wish to crouch and shoot with one key in a FPS-game, but the regular in-game setup only allows separate keys for the task. You might then write a simple line of script that remaps a key to perform crouch and shoot with one press of that key. Another script might automatically reduce the recoil. More advanced scripts create bots[25], which is regarded as a cheat in MMORPGs. For instance, one of the first cheats to appear in the World of WarCraft MMORPG was a fishing bot, a script which allowed the player to leave the game running while the character continued fishing in a lake and gathering experience and resources. Some scripts are allowed and seen as part of the game, whereas others are regarded as outright cheating – but this may be different from game to game and from ladder to ladder.



What this discussion about tweaking and scripting highlighted is the fact that aside from pure hacks, finding a single definition for cheating is impossible at the moment, as the definition of a cheat varies from game-community to game-community, from ladder to

[24] See http://en.wikipedia.org/wiki/Macro, and http://en.wikipedia.org/wiki/Script_programming_language.
[25] Bot is a macro or script which performs a task or a series of task automatically, like aiming and shooting for the player.

ladder and from player to player. Some might be skilled enough to find hidden settings that can be tweaked that allow them significant advantage over their non-tweaked fellows. But since the developer of the game on some level has not forbidden such tweaks by making them possible, the tweakers reason that it can not be a cheat. So instead the community itself regulates the matter, and a form of consensus arises over time. Certain settings and certain tweaks and scripts are considered cheating, and using the tweak is forbidden. The problem is that different ladders may mandate different rules, leading to a splintered community.

2.5 Why do People cheat?

A few years back, I was migrating[26] from one game to the next in the series. A fellow gamer who was thinking about migrating too asked one of us who had already migrated; "Do people cheat in this game?" The answer was as simple as it was obvious; "Do people cheat in the Olympics?" When any large group of humans comes together to play games, be it ordinary games such as sports or board games, or computer games – someone will inevitably find a way to cheat.

Richard Bartle suggested that players who play online multiplayer computer games (MUDs[27] actually, but the categorization could be used for other games as well) fall under one of four different characters: the *socializer* (who play games because he enjoys the company of others) the *killer* (who play because he enjoys harassing and destroying for other players) the *achiever* (who plays to be best, to win) and the *explorer* (who like to explore the games, finding hidden secrets and flaws in the game)[28]. Aarseth suggested that another player category be added to the four – the *cheater*,[29] the player who exploits flaws in the game to his own advantage, even to the point that he uses programs specifically created to allow him the cheats. As to why people cheat in online computer games, that question in itself could probably be the subject of whole psychology or sociology paper. In the limited space allowed here, I will try to list the reasons I think are the most likely, based on my own online experience.

- Be the best

[26] Migrating is a term that means, in this context, switching games. A player migrates from a (usually older) game to a newer one. Frequently the old game and the new are of the same series.
[27] MUD, in the online gaming context, stands for Multi User Dungeon, Dimension or Domain, and is a text based role playing game. I.e. the commands, environments, computer controlled characters and other players are all given and described in text. See http://en.wikipedia.org/wiki/MUD for more information.
[28] Bartle, http://www.mud.co.uk/richard/hcds.htm
[29] Aarseth, P 4. http://hypertext.rmit.edu.au/dac/papers/Aarseth.pdf

I started out this chapter by comparing online games to the Olympics. Obviously online computer games can not be compared to the Olympics just yet, but the principle holds true. Some people cheat to be the best - for the bragging rights and the admiration of other players or perhaps they just can not stand to lose.

- Economic Incentives

There are, however, reasons to cheat that perhaps an outsider can acknowledge more readily. Sometimes sponsored tournaments and cups are held in many RTS and FPS-games, meaning that the winners receive some sort of prize. For example, if a graphics card manufacturer wants to promote the new graphics card that is allegedly excellent for a certain new game, he might sponsor a tournament where the winner receives this new card. Obviously a cheater will have a much better chance of winning. There are also economic incentives to cheat in MMORPGs, as you can sell items and characters you have acquired for real money.

- Destroy the fun for others

When you were a kid, wasn't there some other kid who just loved to smash and destroy for others? Or the latest movie you went to see, wasn't there someone in the audience who just had to break the mood in a crucial scene with a lousy loud comment? Well, these types of people frequent online computer games as well, as Bartle observed. Some of them uses cheats to deliberately destroy the fun for others.[30]

- The paranoia

Someone who assumes that nearly everyone who is better than he is a cheater might start cheating himself just to get even - if everyone cheats, it is only fair that he do it as well, or so he reasons.

- It is fun

Some cheaters argue that they do it simply because it is the best way for them to enjoy the game. They have more fun cheating than playing clean, hence they play in a way that is most enjoyable for them, not caring about ruining the fun for legitimate players.

[30] http://www.myg0t.com Myg0t is a good example; they are a notorious clan dedicated to cheating and aggravating other players. They are mostly known in Counter Strike circles.

2.6 A brief look at the computer gaming industry

The computer gaming industry consists of two major types of actors – the game developers and the game publishers (although sometimes the developer and the publisher is the same company – when in-house studios develop games). The developer is the studio that develops a game. They create the entire game either from scratch or from a license on the games engine. The publisher's skills lie in identifying and financing games that sell and market these towards the distributors and retailers.[31] When the game is finished, the physical copies of the game are created. This is called "going gold", which refers to the actual pressing of CDs and DVDs, the medium on which the game is distributed by to the retailers.

A developer pitches an idea for a game with a publisher, and since creating games is costly and takes time, receives an advance that will keep him going until the game goes gold. The publisher then takes the profit until the advance is covered and then splits the profit with the developer in a ratio depending on the contract. Of course, the costs for creating a game differ wildly. Some games are created with five or six people working full time for a year or two, whereas other games can at times employ 60-100 people over a period of five years. Those big titles are called "AAA", and are expected to sell good worldwide. A "typical" AAA title had a budget around 2 million US dollar in 2001[32], and budgets significantly higher exist.

The personnel involved in creating a game follow an inverted u-curve. The initial size of the staff is small and continues to grow until the game is approaching a state of near completion. At that time most of the staff is laid off and at best, a small team remains to support and patch the game. The continuity in the game developer business is therefore small, as it is difficult for most developers and publishers to eliminate downtime for the personnel in between games[33]. Although the money leak is plugged when the personnel is laid off at the completion of a game, the continued support of the game may suffer. This was adapted to the situation some years back, before the growth of online play, because a game sold most copies the first month it was released.[34] The consumers bought the game, played it and put it away, perhaps a few patches was released closely after the release. With the exceptional success of Counter Strike this was changed. CS attracted new

[31] Kofler. P 26 and forward. http://ep2010.salzburgresearch.at/knowledge_base/kpmg_2002.pdf
[32] Wardell*, P 3, http://www.avault.com/developer/getarticle.asp?name=bwardell4&page=3.
[33] Sawyer, P 9. http://www.avault.com/developer/getarticle.asp?name=bsawyer1&page=9
[34] Hargreaves.* http://www.talula.demon.co.uk/games.html

players long after its initial release and prompted the owner Valve to support the game with updates for, when this is written, five years. Five years is an eternity for a game to survive, especially with such a large fan base that CS enjoys. The online multiplayer community demands constant updating to remain faithful to the game. Crappy support will cause them to leave the game and, consequently, not buy the expansion packs. However, the majority of gamers still buy the games for single player, and the hardcore multiplayer fan base is a minority still. The Entertainment Software Association, ESA, reported that "*43 % of most frequent game players say they play games online",* but that includes simple browser-based games, online trivia, puzzle board games etc.[35]

The hardware manufacturers (those that develops and builds components for PC's) lives in a symbioses with the game developers and publishers. Newer more technically advanced games require more powerful computers to play the game; hence a hit AAA title boosts sales for hardware manufacturers. In fact, games drive the PC hardware industry forward.[36]

[35] http://www.theesa.com/files/EFBrochure.pdf, P 9.
[36] Shim. http://news.com.com/2100-1043_3-5295390.html

Chapter 3: Copyright and the creation of Cheats

The basics of owning a copyright entails the right to prohibit or authorize:

- its reproduction or spreading in various forms, such as printed publication or sound recording;
- its public performance, as in a play or musical work;
- recordings of it, for example, in the form of compact discs, cassettes or videotapes;
- its broadcasting, by radio, cable or satellite;
- its translation into other languages, or its adaptation, such as a novel into a screenplay.

This is called the "economic rights", as opposed to the "moral rights". These rights have a time limit, a minimum of 50 years after the death of the creator (the Berne Convention article 7. Higher limits are possible, the European Union have 70 years). The copyright system, indeed the entire Intellectual Property system is based upon *exclusivity*, the right for the owner of the IP to be the one to decide what should be done with it. Copyright protection is achieved at the moment of creation, without the need for registration[37], as long as the work is original, new and fixated upon some form of media. The fixation criteria is up to individual countries, see the Berne Convention article 1(2).

Copyright was originally created in the 18th century as an instrument to prevent others from spreading the works of a creator of an artistic effort without permission of the author and thereby bereaving him the income he was entitled to for his efforts. This movement, the focus on the rights of the artists, was particularly strong in European continental tradition, and also led to the concept of *droit-moral,* the author's moral rights. The Anglo-American tradition (the common law system in England and USA) instead began as a legislation focused on protecting the investments of publishers and booksellers, leading to a legislation focusing on their corporate needs.[38]

Traditionally, each sovereign nation legislates independently of others. It was recognized early though, that international treaties were required for the copyright legislation to have

[37] Some countries previously demanded registration of a copyright, like the US, but this changed for them when the international treatises were signed. The sign for a registered copyright was ©, which is still used to indicate that the work is protected, although it is not necessary to add the symbol.
[38] WIPO, P 23-25.

any effect. Particularly since some countries did not recognize the copyright of foreign authors, but instead allowed domestic publishers to 'steal' their books and publish them. The Berne Convention (BC) for the Protection of Literary and Artistic Works were signed in 1886, and remain in force today, after several revisions – the latest made in Paris 1971 with an amendment in 1979.[39] The most important clause at the time was the assertion that foreign authors were to be granted the same rights as domestic authors. The BC today, though not obsolete, has been more or less augmented with newer conventions and treatises. A 1967 meeting in Stockholm saw the creation of Word Intellectual Property Organization (WIPO), which is a UN specialized agency overseeing the international treatises. Currently 181 states are members of WIPO[40], and 49[41] have ratified the WIPO Copyright Treaty of 1996, which is a treaty connected to the BC.

Further updating the international obligations, the Agreement on Trade-Related aspects of Intellectual Property Rights (TRIPs) came into effect when the General Agreement on Tariffs and Trade (GATT) became the World Trade Organization (WTO) in 1995. Regulations in TRIPs, according to article 2.2, shall not derogate from previous commitments from the BC, and TRIPS requires members of WTO[42] to accept nearly all conditions in the BC in any case (Article 9, TRIPs).

So to sum it up, international copyright have two major sources:

- The Berne Convention (BC)
- Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs)

Despite the ongoing harmonization of copyright law, laws can still differ from country to country, sometimes even quite significantly. Internal case law, i.e. how domestic courts interpret the law, is of course impossible to control without a supranational court that has the final say (no such court exist, e.g. WTO can only handle complains regarding the trade between nations - and its judgements are merely recommendations that allows the offended country or countries the use of trade sanctions against the offender. The BC was, until brought in under the WTO via TRIPs, even harder to enforce[43]). Countries may also interpret and implement the requirements of international law somewhat differently into their domestic law. However, these international treatises have at least established a norm,

[39] Currently, 157 states have signed the BC. http://www.wipo.int/treaties/en/documents/pdf/e-berne.pdf
[40] http://www.wipo.int/about-wipo/en/members/
[41] http://www.wipo.int/treaties/en/documents/pdf/s-wct.pdf
[42] WTO has 141 members at this time. http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm
[43] Gervais, P 73.

a minimum requirement, which countries must adhere to. This ensures that the basic rules are the same almost worldwide. Of course, this is especially important regarding computer programs – software. Since Internet knows no boundaries, programs and files can spread almost instantaneous between countries and continents. National law becomes more and more irrelevant, since the giants of the industry operates on a global stage, and the pressure of harmonization will in all likelihood continue to grow.

As the name implies, it is the primary purpose of copyright laws to prevent unauthorized copying. But the emergence of other types of copyrightable material (like computer programs) has led to changes and adaptations in copyright legislation as other types of interest have been deemed worthy of protection. The European Union (EU) has in order to have a wholly functional internal market, taken the harmonization effort one step ahead of its international obligations. Several directives have been issued, and important regarding computer software is:

- Council Directive 91/250/EEC on the legal protection of computer programs. (The EU Software Directive.)
- Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society. (The 'InfoSoc Directive' or the EC Copyright Directive.)

3.1 Copyright and Computer Programs

Copyright does not protect the underlying ideas and methods, rather the *expression* of ideas[44]. Two people can gain copyright from their individual expression of the same idea, so long as one is not a copy of or too alike the other. A certain amount of originality and creativity is required to gain protection; your average doodling by the phone will in all likelihood not be copyrighted.[45]

An author of a book would normally expect his readers to perceive and appreciate his ideas and thoughts – after all, that is the point of books. A computer program however, is a different matter. Proprietary software[46] usually contains ideas and methods the company wishes to keep secret, and the user is not encouraged to ascertain underlying ideas and principles. Sometimes the ideas and methods in computer programs are even

[44] Article 9(2) (TRIPs). See below for the article quote.
[45] Anawalt et. al. P 1-77.
[46] As opposed to "Free Software". The terms "Open Source/Closed Source" are also used frequently – see http://www.opensource.org for more information on open source.

heavily protected with encryption and obfuscated code[47]. This opposed to the patent system, where ideas and methods can be protected. Thus the copyright system is considered a weaker protection than the patent system,[48] and heavy lobbying from the industry has resulted in a glide from pure copyright protection for computer programs to include the possibility of patent protection as well. Originally, programs were considered not patentable, but a phenomenon called pure software patents have emerged lately in the US, and may be on the way in Europe as well. This development is beyond the scope of this essay.

Computer programs are written by programmers in a high level computer programming language[49], which is human readable to those who know the programming language, and called *source code*. This source code is then transformed with another program, a *compiler,* into *object code* which is machine readable since it consists mostly of machine code in the form of binaries, 0s and 1s the computer can read and understand. It is the source code that companies wishes to keep secret, but with the help of programs called decompilers, users can *decompile* the object code and transform it into source code, thereby being able to investigate the inner workings of a program – a process sometimes referred to as reverse engineering. So companies generally wants to limit the users ability to gain access to source code, as solutions the company wishes to be kept secret can be deduced from studying the source code.

When computer programs began to emerge, there was uncertainty as to if and how they should be protected. The intellectual property that seemed closest to the concept of software was copyright, so most nations opted to include software in the protection granted from copyright,[50] which was more of a policy decision since drafting a new law would take more time than available due to the pressing need for a protection.[51] The first multilateral treaty to include computer programs explicitly in the protected area was TRIPs[52];

[47] Obfuscated code is a way of writing code intended to make it difficult for a person to discover the underlying principles in the source code. http://en.wikipedia.org/wiki/Obfuscated_code
[48] Anawalt et. al. P 1-78.
[49] Or more rarely, a low-level programming language, called "Assembly language". The human readable form is translated into object code with an assembler and the reverse by a disassembler.
[50] Gervais, P 80.
[51] Stamatoudi, P 157.
[52] The TRIPs text here and below has been cut to include the relevant parts only. The TRIPs agreement in its entirety can be found at: http://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

Article 10 (TRIPs)
1. Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971).

There had been some debate as to whether the artistic expression as a literary work resided in the source code only, or in the utilitarian object code as well[53], which was dispelled with this section. Although article 10 specifically mentions computer programs as protected, it gives no clue to the extent of that protection. The exclusion of certain elements not protected can be found in article 9(2) of TRIPs;

Article 9 (TRIPs)
2. Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.

This does not give us much information either, as I said above ideas and such is not protected under copyright laws. Compared to article 2(1) of the BC an exclusion of objects is mentioned for the first time internationally, as 2(1) enumerates a non-exhaustive list of objects protected. However, for more specific boundaries of protection for computer programs, one has to turn to other sources.

3.1.1 Are videogames protected by copyright?

Videogames (games) are certainly a form of computer programs. They are written in source code and transformed to object code just as other computer programs, and are thus protected under the copyright laws according to article 10(1) of TRIPs in both code forms. The question is rather if games can be protected as audiovisual works as well. The audiovisual part refers to the game play, i.e. the movies displayed on the computer screen, the music, and the sound effects etc. and are dependant upon his actions. Stamatoudi argues that the computer program of a game is merely the technical part which facilitates the visual effect[54], that of playing the actual game and the images brought to the user on the monitor. The point is that protecting only the computer program part of the game leaves the audiovisual parts more open to infringement, so a copyright protection should extend to all parts of a game – i.e. including everything of a multimedia work that is original and new. Thus, a game that can qualify for protection both as computer program and an audiovisual work will receive a stronger protection than a game protected as a

[53] Gervais, P 80.
[54] Stamatoudi, P 156.

computer program only. Recent case law confirms this[55], as games nowadays are seen by courts as both computer programs and audiovisual works "in most countries".[56] This includes the USA[57], which had a number of significant court cases regarding computer software. Isolated occurrences, like a single sound effect, are most likely not copyright protected as separate works[58], it is rather the combined effect that is protected.

This means that if someone writes a game with a completely different source code than any given game, but creating a game that closely resembles that game when seen on screen, an infringement has been made. The on screen result is as protected as the source code. This may sound self evident, but initially games were denied protection altogether due to a perceived lack of fixation and originality. Later, they were only protected as computer programs as the originality criteria were thought not to be fulfilled as the "movie" is the result of interactivity leading to different images all the time,[59] there was even suggested that the player took part of the creative process and should be considered co-creator. The logical answer was of course no, as the player only can generate images whose potential already existed in the programming of the game and were, to some extent, predicted by the programmers.[60]

3.2 How are cheats created?

To investigate the extent of copyright protection when it comes to cheats that are created for games (hacks), one needs to understand a bit on how cheats are created. An online multiplayer game can be designed in two basic ways, called client-server and peer-to-peer.

The client-side architecture means that each player has a client that communicates with the server, i.e. the client takes the input from the player and sends it to the server. The server has control over all information in the game and sends back the information relevant to the client based on the players actions. At any given time the client, the player's computer, only have access to a limited amount of information from the game.

[55] Case law can of course vary from country to country, but note that some if not most countries does not have any significant case law on copyright and videogames.
[56] Stamatoudi, P 178.
[57] Anawalt et. al. P 1-111.
[58] Stamatoudi, P 179.
[59] Stamatoudi, P 168-176.
[60] US Court Case: Williams Electronics Inc v. Arctic International Inc., 704 F.2d 1009 (7th Cir.), cert. denied, 464 U.S. 823 (1983).

This means that the server runs the game and chooses what to tell the client. Client-server based games needs to be played on a server, dedicated or non-dedicated. Most FPS games and MMORPGs are client-server based, and some RTS games.

Peer-to-peer (P2P) operates without an independent server, and the information from the players computers are not relayed via servers. Instead each player's computer has access to all pertinent information at any given time, and information is sent directly from computer to computer. Many of the (in)famous file sharing networks rely on peer-to-peer architecture. RTS games are usually built as peer-to-peer based games.

Peer-to-peer based games are extremely hard to protect against cheats. Since each player has access to all information, even all the data about the other players, he can change it on his computer at will, albeit some effort and skill is required to create hacks, and the other computers in the game will simply receive that information and act on it. Anti-cheat efforts in P2P are based on comparing every computer with each other regularly, and assuming that the odd computer that does not behave like the others is cheating. However, the anti-cheat method used in P2P based games can only be based on soft values - appreciations, not absolutes, since every computer acts differently e.g. due to the latency. The computers are never or very rarely fully synchronized.

This problem is somewhat reduced in client-server based games, as the server will hold most of the information. But as the common maxim among multiplayer game designers say: "Never trust the client".[61] Every piece of information sent to the client from the server, and every piece sent back, is subject to cheat exploitation. These cheats are based upon the actions of the client alone and are thus not as extensive as in peer-to-peer based games as data about the other players are kept server-side. In both game types, game developers try to limit the usability of information with encryption and obfuscated code and so on, but the possibility of reverse engineering always exists. Furthermore, some cheats does not even require that the main program (the game) is altered. So even if client-server is to be preferred from an anti-cheating perspective, information on the player's computer is still vulnerable. For example, a wallhack in a client-server based game can not be perfect in the sense that other players can be tracked all over the map. But as soon as another player is within the reach of when the server needs to tell the client the whereabouts of that player, the wallhack will reveal the other player.

[61] http://en.wikipedia.org/wiki/Cheating_in_online_games

There is also a trade-off in anti-cheat methods. Lesser information trusted to the client will result in higher strain on the server and the Internet connections of the clients – and the performance of the game will be affected adversely. Going too far in anti-cheat design may result in game that is virtually unplayable. The harsh truth is that to date, all cheating can not be stopped. One can simply not control the client to the extent needed[62], and some cheats can not be distinguished from how a client normally behaves; a good player can sometimes appear to be as fast as an aimbot.

So then, how are cheats actually programmed? This is a list of examples (based on this article[63]) that each illustrates a different point about cheat creation;

- Hard-coded Hack

The simplest of cheats, this technique replaces the game's files with modified files that enable cheating. Replaced files can be .dll and config-files. These types of cheat directly modify the game's software.

- Driver Hacks

OpenGL (stands for Open Graphics Library) and Direct3D are applications involved in the graphics card drivers operations. These drivers can be modified outside the game so they draw the in game structures differently, like enabling a wallhack. In fact, a few years back a prominent graphics card manufacturer released a set of drivers that explicitly (i.e. without the need to hack the software) allowed manipulation of textures in game allowing transparency and wireframe modes. The outcry from the gaming community however, caused the company to withdraw the set of drivers with that feature. This type of cheat does not actually have to modify any game files, but instead focuses on other software that process information from the game.

- Client Hook

This cheat allows the player to load up a "client-loader" or an "injector" when the game is started, and injects lines of code directly into the RAM, which allows the game data sent to and from the server to be manipulated directly in the memory, bypassing the game

[62] This client-monitoring also raises issues concerning privacy and integrity, as to what extent is it acceptable to spy on player's computer to prevent cheating? This, however, is a subject for another paper.
[63] Moses, P 2. http://www6.tomshardware.com/game/20030517/index.html

itself. This hack does not change the permanent game files, but rather the copies of game files done in the RAM necessary to run the game.

3.3 Modifications

Recent years has seen an explosion of a phenomenon called mods (short for modifications) in the gaming industry that resembles the open source movement in some aspects since they are released free of charge and involve the general public in the development. Some mods actually become open source projects. Mods are alterations of games, and can range from everything as simple as adding new gun to something complex as creating a totally different game. Mods are either partial conversions or total conversions, partial conversions being basically expansion packs to the original game, whereas total conversions are for all practical purposes a brand new game. The rule of thumb is that editing some elements of the game while leaving the better part of the game play intact results in a partial conversion. Obviously, total conversions are rare as they are huge projects that require significant amounts of man hours. Although the game developer paved the way, a lot of work still needs to be done in order to create, in essence, a new game. Mods are mainly created for RTS and FPS games, the control over the servers the developers maintain in MMORPGs means that any modifications to the game play are regarded as hacks. Other game types do not have a sufficient customer base to generate much interest in mods, although exceptions probably can be found.

Ever since the smash hit Counter Strike, the industry has realized the value of having mod makers as a part of their gaming community. Counter Strike was initially a multiplayer only total conversion mod for the game Half Life featuring a totally different game play. The success was so big that the developer of Half Life (Valve) eventually made the game in a stand alone retail version (the game can still be downloaded free if you own a copy of Half Life) and later released a semi-new game called Counter Strike Condition Zero that is purely retail. The point is that mods spawn interest in the original game, perhaps prolonging the lifetime of the game, and since mods can not be played without the original game people will still buy the original. Thus developers allow and even encourage mods, even though they can be, in a sense, violations of copyright laws; [64]

[64] The convention text here and below has been cut to include the relevant parts only. The Berne Convention in its entirety can be found at: http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html.

Article 12 (Berne Convention)
Authors of literary or artistic works shall enjoy the exclusive right of authorizing adaptations, arrangements and other alterations of their works.

Mods can thus be seen as *dependant* or *derivative* works, meaning that they are so closely related to the original copyrighted work that they require the permission, authorization, from the original copyright holder (see also article 4(b) from Directive 91/250/EEC below). However, the territory of copyright, modifications and add-ons to computer software is legally unexplored, to say the least. For instance, it is also possible to argue that some mods and add-ons constitute a new, non-derivative work. Compare this situation with a program being created to run on the Windows platform – nobody would argue that Microsoft have the right to authorize all the programs that can run on their operative system simply because they are compatible with it. The same can be said for a mod that simply is made to run on a certain game-engine. The outcome largely depends on how much the mod-maker relies on the earlier work done by the game-developer – incorporating large sections of code would almost certainly make it a derivate work, whereas simply designing something to run on a certain game engine would not.

Note that the mod makers still have the copyright to *their* mod, irregardless of whether it is derivative or not (unless otherwise has been agreed[65]);

Article 2 (Berne Convention)
(3) Translations, adaptations, arrangements of music and other alterations of a literary or artistic work shall be protected as original works without prejudice to the copyright in the original work.

Although the modder (mod-maker) still need the permission of the original copyrightholder to release their mod, if it is a derivate work. Which developers and producers gladly give, even to the extent that specialized mod making tools are released. These are called Software Development Kits (or SDKs), and comes with a special license stating what the mod makers can and cannot do.

There is a big difference between mods and cheats. Cheats are almost always covertly used, but most importantly – they are one sided. Cheats aim at giving the cheater an unfair advantage over the other players, something that fair players normally do not have access to. Mods are openly advertised as such, and in order to play a modified game the

[65] More information about agreements, mandatory and non-mandatory laws can be found in Chapter 5.

player needs to download the software containing the mod. When he wants to play the modded game, he needs to find servers and/or other players with the same mod installed. So the field of play is level since everybody must play under the same conditions given in the mod, just as in the original game, and mods are permitted by the copyright owner, unlike hacks.

It can, however, be argued that the more information about a game that is given to players, the bigger the risk for cheating and hack creation is. When the source code for Quake 1 was released a few years back it elicited a heated debate when gamers realized that access to source code simplified the work for the cheat creators.[66] Similarly, cheat codes and other "easter eggs" provided in single player games simplify the cheat creation process.[67] SDKs do not contain any significant amount of source code, although samples of it can be bundled, as well as explanatory manuals and other tools helpful to mod makers. In any case, it can be argued that SDKs that allows people to play around with the software simplifies the cheat creation process. Although it should be stated that crackers will create their cheats with our without SDKs, as proved by several games released without SDKs but with plenty of hacks. However, this debate caused well known open source spokesman Eric S. Raymond to argue in favour of open source games as a method of stopping cheats.[68] Open source code, he argued, will force the developers of the game to secure the game against all possible hacks against a cracker with full insight into the system – a security a professional cryptographer can respect. It may be so, but the problem with his idea is of course that the companies wish to keep their solutions secret. If the source code was routinely released competing companies would copy their work with minimal effort. It is not for me to say which system, open or closed source, is for the best, and it is not within the scope of this paper to examine the ongoing debate. However, no successful attempt has been made to create a *major* open sourced game with protection along the lines of Mr. Raymond's ideas – at least to my knowledge, and perhaps this is what is needed to achieve better protection against cheats. But the fact that no attempt has been made during these five years since his article were published also tells us that no one thought it was worth a try, at least not among the major game developers or publishers.

---

[66] Carmack, http://www.bluesnews.com/cgi-bin/finger.pl?id=1&time=19991226003141. John Carmack is the near legendary co-creator of FPS games such as the Doom and the Quake series, see http://en.wikipedia.org/wiki/John_Carmack for more information.
[67] Pritchard, http://www.gamasutra.com/features/20000724/pritchard_pfv.htm
[68] Raymond, http://www.catb.org/~esr/writings/quake-cheats.html

The modding-community highlights both the negative and the positive sides of computer gaming, a part that is both its strong and weak side. On one hand, the personal computer architecture allows players to modify games to suit their own needs, even to the point so that they can create new games based on the old that may be more fun to play than the original. On the other hand, computer games allow cheat-creators to modify game files and create auxiliary programs that enable hacks destroying the fun for other players.

3.4 Alterations of Copyrighted software – the European Union

As I stated above, copyright protection for software came rather late in the development of copyright and seemed to fall into the middle of copyright and patent protection. The problem has e.g. in the European Union been targeted with special legislation (Directive 91/250/EEC), changing the copyright laws to accommodate and address problems specific for computer programs.
Article 4 in the Directive restricts the user from certain acts;[69]

Article 4 Restricted Acts (Directive 91/250/EEC)
Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2, shall include the right to do or to authorize:
(b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;

The meaning of the article is clear; it is not allowed to change a computer program, like a game, without the permission of the rightholder. This main rule, however, have some exceptions;

Article 5 Exceptions to the restricted acts (Directive 91/250/EEC)
1. In the absence of specific contractual provisions, the acts referred to in Article 4 (a) and (b) shall not require authorization by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.

3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while

[69] The Directive text here and below has been cut to include the relevant parts only. The text in its entirety can be found at: http://europa.eu.int/ISPO/legal/en/ipr/software/software.html.

performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

Thus we can infer that you *only* have the right to alter a game when it is *necessary* to alter it so it can perform its intended, 'normal' operation, such as alterations to make the program run on your specific hardware, achieving interoperability with other software and the fixing of bugs. You also have the right to study the program to ascertain ideas and principles behind it. This means (unfortunately, in this case) that a cheat creator may legally observe the program in order to find possible exploits.

You are also allowed to decompile, access the source code, a software program, if it is done to achieve interoperability with another program;

Article 6 Decompilation (Directive 91/250/EEC)
1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs

2. The provisions of paragraph 1 shall not permit the information obtained through its application:
(a) to be used for goals other than to achieve the interoperability of the independently created computer program;
(c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

This could be interpreted to mean that a cheat creator who has a program allowing cheats wishes to achieve interoperability with the game can decompile it in order to do so. However, the information may not be used for any act that infringes the copyright of the original program (2 c), like altering it without permission, and thus decompiling in order to create hacks is an infringement of copyright.

I submit that creating cheats is a clear violation of the copyright. Hacks alter or adapt the game without the authorization of the rightholder (unlike mods). Hacks that do not alter the actual game software may also fall under the protection afforded by the Directive, since they at least alter the final input on the players screen. As we saw in Chapter 3.1.1 above, the audiovisual parts of a game are copyrighted and are thus subject to the same protection under the Directive. Regarding the exceptions to this restriction, I am convinced that enabling cheats in the multiplayer part of the game can in no way be seen

as step in ensuring that it is performing its normal operations. In fact, hacks are the opposite of the "intended purpose" in multiplayer games. It is also forbidden to distribute programs that enable such alterations ("the reproduction of the results" Article 4(b) above). Nevertheless, it is possible to argue the opposite. Hacks that do not incorporate any parts of the game itself may fall beyond the scope of copyright altogether – like programs created to work on operative systems does not give the operative system's owner any rights to such programs.

3.5 Alterations of Copyrighted software – the United States

The EC Directive is of course only valid within the European Community, and the situation in the US is somewhat muddier. The extent of allowed alterations and such uses for software is basically governed by the same principle as found in the Berne Convention article 12, which states that the author, (or copyrightholder) has the exclusive right of authorizing adaptations, alterations and such, meaning that derivative work falls under the copyrightholders control (United States Copyright Act § 106:2) and are thus infringements if no permission is obtained. The scope of this basic principle is in the US regulated by the doctrine of fair use.[70] In connection with fair use, there has been a debate whether reverse engineering and decompilation is fair use or not[71], which it now is, although the debate rages on[72]. The question of altered software in the US seems to be that it is not allowed if it can be seen as a derivative work. (Note that a copyrightholder has the right to restrict users from reproducing and creating derivative works in *both* a public and private context[73].) Douglas L. Rogers describes the problem;

"An alleged infringing work must incorporate the original work in some fashion in order for it to constitute a derivative work. For instance, in Lewis Galoob Toys, Inc. v. Nintendo of America, Inc., the Ninth Circuit concluded that a program that increased the number of lives of the game player's character, increased the speed at which that character moved, and allowed the player's character to float over obstacles, did not create a derivative work. The court noted that the Game Genie (the add-on program that caused the changes) blocked values sent by the Nintendo cartridge and substituted new

[70] United States Copyright Act, § 107. The text is omitted or cut, the entire act can be found at: http://www.copyright.gov/title17/.
[71] See for example Karjala, http://homepages.law.asu.edu/~dkarjala/Articles/DaytonLRevSpring1994.html.
[72] Anawalt et. al. P 1-118.
[73] See for example the FAQ question "What rights are protected by copyright law?" here; http://www.chillingeffects.org/piracy/notice.cgi?NoticeID=1408#FAQID12054

values, but did not incorporate a part of the copyrighted work in a concrete or permanent form. In other words, the Nintendo cartridge did not perform as expected/desired by Nintendo, but the court concluded that the Game Genie did not create a derivative work. Just as a derivative work is not created when an individual points a kaleidoscope at artwork, Game Genie did not create a derivative work."[74]

This case seems at a superficial glance to condone outright cheating. An analysis, however, raises the question how valid it is regarding the situation at hand; cheating in online multiplayer computer games. First of all, the case concerns a console game and the cheats were added using a cartridge. Granted, the case seems to state that a cheat who do not *permanently* incorporate the copyrighted work in the cheat program is allowed. But to contrast this, the case Midway Mfg. Co. v. Artic Int [75], concerned a chip that sped up the rate of play and was seen as a derivative work and thus an infringement. Secondly, the case was regarding singleplayer cheats. Cheats in multiplayer games today does not affect the player only, but has a detrimental impact on *other* players whose copies of the game are clean from cheats. Singleplayer cheats are common and more or less the business of individual players, whereas as multiplayer cheats are frowned upon in the industry. Thirdly, the case is from 1992, over a decade old. The development of computer gaming and the economic impacts of multiplayer cheating have led to a totally different situation. Much of the reasoning in Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.[76] concerns the impact of the alleged infringement on the market. Multiplayer cheats today have a totally different impact on the market, detrimental to game developers and producers as customers flee cheat-infested games, which may very well affect the scope of the fair use doctrine regarding alterations of computer games. The incorporation of the original work was *temporary* in Midway Mfg. Co. v. Artic Int, but affected the copyrightholder's revenue from the temporary incorporation. Multiplayer cheats today affect the revenues of copyrightholder's, a strong argument for considering cheats as infringements.

The § 107 outlines four principles that US courts should take into account when deciding whether a use is fair or not. They are:

[74] Rogers, http://www.vssp.com/CM/Articles/articles794.asp.
[75] Midway Mfg. Co. v. Artic Int'l, Inc., 704 F.2d 1009 (7th Cir.), [**9] cert. denied, 464 U.S. 823 (1983).
[76] Lewis Galoob Toys, Inc. v. Nintendo of Am., Inc., 964 F.2d 965 (9th Cir. 1992), *cert. denied*, 507 U.S. 985 (1993).Case found at; http://cyber.law.harvard.edu/openlaw/DVD/cases/Galoob_v_Nintendo.html

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

Some cheats are actually sold for money which definitively will affect the fair use ruling; Campbell v. Acuff-Rose Music, Inc[77], *"every commercial use of copyrighted material is presumptively an unfair exploitation of the monopoly privilege that belongs to the owner of the copyright."* Nevertheless, there are no legitimate uses for creating cheats and release them for free or keep them private either. In American Geophysical v. Texaco, Inc.[78], it was stated that *"courts are more willing to find a secondary use fair when it produces a value that benefits the broader public interest."* I would argue that hacks are just the opposite; they produce programs that are detrimental to the public interest, i.e. the majority of those who play the game. (See Chapter 3.3 above for an explanation why benign modifications are allowed – mods.)

(2) the nature of the copyrighted work;

The game software and the audiovisual qualities produced thereof aims at one goal; the player shall enjoy playing the game so they buy it, its expansion packs and sequels, pay subscription fees etc. The nature of the multiplayer part of the game is to ensure a level field of play where everybody can play and compete on the same terms (notwithstanding Internet connection and computer hardware). Hacks change this equilibrium.

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

Cheats does not as such use or incorporate the copyrighted work in any substantial amounts, they are small programs or alterations of game files that changes the audiovisual appearance. This speaks for fair use.

(4) the effect of the use upon the potential market for or value of the copyrighted work.

As I have said a couple of times already, cheats affect the market detrimentally for the game and speaks heavily against a fair use exception for hacks.

The law is not written in stone, it is ever changing and adapting to new circumstances. A good lawyer is able to use and present the law with persuasive arguments to the maximum benefit of the cause he is representing, even causing the court to reinterpret the law, or in a sense creating new law. Copyright and cheats in computer games is an example of this, the field is so new and evolving so quickly that no one can, with any

[77] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 584 (1994).
[78] American Geophysical v. Texaco, Inc., 37 F.3d 881 (2d Cir. 1994).

great certainty, say what the law is (de lege lata). The chapters above (3.3 - 3.5) represents a line of reasoning, a theory, that cheating violates copyright laws – what the law should be (de lege ferenda). That does not mean that a judge would agree and until a court ruling clarifies the issue, one can only speculate. It is nevertheless my opinion and belief that the creation and use of hacks are copyright violations both in the European Union and the United States.

3.6 Moral Rights and Cheats

The moral rights began as the attempt to protect the "romantic" ideals of artistic integrity and aesthetic achievements, aside from the more harsh reality of the practical economic rights inherent in the copyright system. Creator of works was deemed worthy of protection even after they gave up the economic rights of their creation, essentially to be able to prohibit misuse of their work. National laws differ over what moral rights entail exactly, i.e. how extensive the protection is, but all or a few of the following bullets are probably incorporated in every legislation protecting moral rights[79];

- A right to decide upon first release.
- A right to be named as creator or co-creator.
- A right to object to modifications of the work.
- And the right to object to presentations of the work in derogatory circumstances.

The Berne Convention incorporated this article regarding the moral rights, which includes the three last bullets above;

Article 6bis (Berne Convention)
(1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.

It should be noted that TRIPs article 9(1) explicitly states that Article 6bis of the BC is exempted from the TRIPs. This means that everybody who has signed the BC treaty is bound by the article, but that it can not be brought under the stronger enforcement system of the WTO if a nation fails to comply with it. The reason for this was that the US

[79] Cornish, et. al. P 444.

admitted that it wanted to "avoid any possibility of these rights being strengthened."[80] That said, what needs to be pointed out is that the main argument against moral rights is its "unwaivability", i.e. that it is not possible to agree that the moral rights are void. The BC does not state that the moral rights can not be waived; instead the treaty makes it clear in articles 6(2) and 6(3) that other questions such as waivability is up to the national legislation.

The Anglo-American system has had a long tradition of suspicion against moral rights, for the reason that any restriction placed upon the investor (i.e. the one who ends up with the economical rights, like a publisher of books) will impede his ability to exploit the work on the market-place by subjecting his actions to some higher ideal. Since the US ratified the BC, they have moral rights incorporated into their legislation (§ 106a of the United States Copyright Act), although it can be discussed as whether they actually meet the conditions of the BC[81]. The moral rights are not transferable, but are waivable under § 106a.

The economic rights of software pass from employee to employer automatically in some jurisdictions[82], or lacking such legislation a clause stating the same is normally incorporated in the employees' agreement. The issue of moral rights, however, are more delicate regarding computer programs and thereby video games. A lot of people can be involved in the creation, as many as hundreds of contributors for some games, and the mess would of course be considerable if individuals started to ascertain the rights too liberally and frivolously object to the exploitation of the software. The moral rights were originally intended for single authors or artists, or perhaps a mere handful having joint ownership. Therefore the employers of the software industry prefer that the employees waive their moral rights or have them transferred to them, if possible under that legislation. But another path is definitively viable and, in my opinion very reasonable; the Swedish legislation states that both the moral rights and the economic rights pass on to

[80] Gervais, P 72.
[81] Koktvedgaard et. al. P 149.
[82] *Article 2 Authorship of computer programs* (Council Directive 91/250/EEC on the legal protection of computer programs)
3. Where a computer program is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the program so created, unless otherwise provided by contract.

the employer regarding computer software. (A so called *cessio legis,* a complete transfer, was intended with the word "transfer" in article 40a.[83])

What is the point of all this then, what does it have to do with cheating in online multiplayer games? Moral rights entitle the author of a work, or the one who holds the moral rights, to object to modifications and derogatory treatment in his work. Traditionally this has been regarding ethical values, like having the right to object when a pornographic movie is based upon your book or having neo-Nazis using your painting as propaganda for their political aspirations. The game developers work hard to develop a certain look and feel, a game play for their multiplayer part of the game (or indeed for the whole game), basically a way in which the game was intended to be played. John Carmack referred to cheating in mp-games as breaking the *spirit of the game.*[84] I claim that creating, spreading and utilizing hacks for a game violate the authors' moral rights, as the use of hack alters the game play derogatory. This statement is, to my knowledge, not tested in courts. However, I find that it is not unreasonable to interpret the law in that way. Considerable efforts have gone into tweaking and perfecting the game play to create a level field of play that the players can enjoy. Creating programs or alter the game files that disturbs this equilibrium where skill should reign supreme destroys the efforts of the developers.

I established earlier (Chapter 3.1.1 above) that games can be protected both as computer programs and as audiovisual works. This is important to realize, as cheats can be created that actually does not change the game files themselves, but only how the game is displayed on screen (e.g. driver hacks). The moral rights protection of the copyrighted work thus extends to the audiovisual parts as well.

This approach, actually using the moral rights as way to stop hacking games for cheats requires a new way of thinking regarding the droit-moral, particularly in jurisdictions where the moral rights are routinely waived or firmly in the hands of individuals (unwaiveable and/or not transferable). Used right, they can become a tool rather than an obstruction for game-developers and -producers that combat cheats. However, this tactic requires that the holder of the economic rights (developer/producer) gathers the right to the moral rights as well. It is probably possible for individual programmers to handle the

[83] Koktvedgaard, P 148. A translation to English of the Swedish Copyright Act can be found here: http://www.wipo.int/clea/docs_new/en/se/se052en.html
[84] Carmack* (you have to scroll way down): http://slashdot.org/article.pl?sid=99/12/26/1255258&mode=thread

issue, but the transaction costs will in all likelihood be huge even if some collective effort is undertaken. Of course, if the moral rights are waived in the sense that no moral rights to the game exists at all there is nothing to be done, but if they are waived towards the employer only the possibility for action still exists.

Chapter 4: Trademark issues and the spreading of Cheats

Unlike copyright, the trademark system is primarily built upon registration.[85] Like copyright, it was recognized rather early on that national protection did not suffice, in fact the first known trademark counterfeiting dates back to Roman times when the pottery trademark FORTIS were copied.[86] In order to grapple the problem of international trademark infringements treatises that outlined common rules and the possibility of applying for trademark protection in other countries were drawn up. The basics are still the same – a trademark needs to be registered *in the country* if any protection is to be achieved[87] – but the treatises simplified this process and ensured that harmonized rules were used.

The Paris Convention for the Protection of Industrial Property came into being 1883, and was revised several times, the latest being made in 1979.[88] 169 countries have signed the convention[89]. It did not contain any procedures for international registration of trademarks, but the Madrid Agreement that came soon thereafter (1891) did. The Madrid Agreement was in 1989 given a protocol, the Madrid Protocol with some changes to the Agreement, which brought in some previously reluctant countries under the Madrid umbrella. Currently, 77 states have signed the Madrid Agreement and/or the Protocol,[90] including the United States and the European Union on behalf of its member states. The TRIPs agreement includes trademark articles as well as copyright articles, and is also an important source of international legislation for trademarks. The European Union have harmonized the trademark system under the Community Trademark (CTM) which is linked to the Madrid Agreement.[91] I shall not go any further in describing the rather

[85] There is a slight difference between common law countries (the Anglo-American system) and civil law countries (e.g. most parts of Europe), since common law countries may demand that the trademark has been used before allowing the registration. See 15 U.S.C. §1051. The American legislation concerning trademarks can be found at: http://www.uspto.gov/web/offices/tac/tmlaw2.html#_Toc52344284
[86] WIPO, P 183.
[87] This is only half of the truth though, well known trademarks can achieve protection with use only, i.e. without the need for registration.
[88] You can find the Paris Convention here: http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html.
[89] http://www.wipo.int/treaties/en/ShowResults.jsp?country_id=ALL&start_year=ANY&end_year=ANY&search_what=C&treaty_id=2.
[90] http://www.wipo.int/treaties/en/documents/pdf/g-mdrd-m.pdf. The legal texts of the Madrid system can be found here: http://www.wipo.int/madrid/en/legal_texts/
[91] See http://oami.eu.int/en/ for more information.

complicated system of trademark registration. Suffice it to say that no world mark exists, applications must be designated to individual countries and achieve protection there, even though the international treaties simplify this process significantly, and that the basic rules of trademarks are the same for most of the world.

It is possible to establish reputation for a trademark, and achieve protection without registration (e.g. when registration is refused due to lack of distinctiveness)[92]. It is therefore some names are followed with the symbol ™ which stands for an unregistered trademark in use. A registered trademark is designated with the symbol ®. Trademarks can, unlike copyrights, last forever as long as the registration is renewed or the mark remains in use and is sufficiently famous.

The definition of a trademark lies in its ability to be *distinguished* from other trademarks;

Article 15 (1) (TRIPs)
Any sign, or any combination of signs, capable of distinguishing the goods or services of one undertaking from those of other undertakings, shall be capable of constituting a trademark.[93]

Therein lies a demand that the trademark must be *distinctive.* For example, a company selling fruit will have a very hard time protecting the trademark "Apple" since all fruit sellers' sells apples and are free to use that name. However, a company selling computers can use the name "Apple" since apples are not connected to computers at all and it is therefore very distinctive in that context.

Trademarks can be used for goods as well as services, and are sometimes named *"service marks"* when used for services. Since any sign, capable of distinguishing goods from other goods is eligible for registration; one can imagine a variety of possible combinations. The most common trademark is of course the word mark, consisting of a name, a sentence or a slogan. Any colour, font, device, drawing etc. can be used for a trademark, thus comprising a logo. Other possible trademarks include three-dimensional signs, audio signs and olfactory (smell) signs.[94] The protected element is the registered mark, naturally. In the case of word marks for example, any use of the same words in any context may constitute an infringement – whether the same font, logo etc. is used or not is irrelevant since the protected element are the words. If a special logo is used together

[92] See Article 15 (1) TRIPs.
[93] The text is cut, the full version can be found at http://www.wto.org/english/docs_e/legal_e/27-trips.pdf.
[94] WIPO, P 186.

with the word mark, or the word mark is also a logo the protection is twofold. Not only is it forbidden to use the words, but also to create a logo with different words but with the same logo (like the same fonts, the same colours and so on) if it is deemed to similar to the already registered trademark.

Trade names are similar to trademarks, with the difference that they distinguish an enterprise – the company – from other enterprises. They are protected with use[95] if they are distinctive enough, and can also be registered as trademarks. For the purpose of this paper, I will refer to trademarks, service marks (if applicable) and trade names as "brands", as the same rules for the purposes of this paper applies to all three.

The basic protection of a trademark is that you can prohibit other from using that mark or one confusingly similar for the *same class of goods or services for which the trademark is registered*. Someone selling t-shirts can not stop someone selling computer software from using the same name, unless the registration covers computer software as well. The exception to this rule is well-known marks, which may be given protection extending beyond the goods or services for which they are used[96]. The Nice Classification system[97] is widely used to categorize different goods and services into classes. The use of the trademark must be "in the course of trade" to constitute an infringement, besides being identical or confusingly similar. It must also be likely to cause confusion amongst customers, which is *presumed* when the trademark is identical and used for the same goods or services.

Article 16 Rights Conferred (TRIPs)
1. The owner of a registered trademark shall have the exclusive right to prevent all third parties not having the owner's consent from using in the course of trade identical or similar signs for goods or services which are identical or similar to those in respect of which the trademark is registered where such use would result in a likelihood of confusion. In case of the use of an identical sign for identical goods or services, a likelihood of confusion shall be presumed. The rights described above shall not prejudice any existing prior rights, nor shall they affect the possibility of Members making rights available on the basis of use.

[95] Article 8 of the Paris Convention.
[96] Article 6bis of the Paris Convention and Article 16 (2) and (3) of TRIPs.
[97] http://www.wipo.int/classifications/fulltext/nice8/enmain.htm

The confusion criterion is largely aimed at individualizing a product for the customer, so that he knows who is responsible for the product.[98] Thus the proprietor of mark does not own the mark in the same sense as owning a copyright, and can not control the use of the mark beyond commercial use in limited geographical areas (where it is registered or well known) and for certain types of goods and services. However, the concept of Intellectual Property (IP) and its role in the emerging information society has led to other interests emerging. A modern company realizes that the brand is their primary communication channel with the customers and that every incident will be connected to their brand. Brand management have thus become more and more important for every type of company, not only those "selling lifestyles". This has in turn led to a different view on brands and how they are used. A good company in this regard will have detailed brand policies on how and when their brand should be used. For example, if a company started making cheap CD-players and began calling them 'Rolls-Royce' the brand Rolls-Royce would decline in value, as it begins to be connected to cheap merchandise. (This has led to the "well known" trademark protection, see note eleven). Thus companies wish to exert as much control over their brands as possible, which, given the law today, is not always possible.

Several legislations have also incorporated fair use exceptions regarding trademarks. For instance Article 12 of the Council Regulation 40/94 on the Community Trademark,[99] which allows spare parts manufacturers to use the trademark for which the parts are intended to fit. Another example is journalists, who naturally are allowed to use the trademarks of the company they are writing about, even though it is in the course of trade (after all, they sell newspapers). However, these exceptions are designed to accommodate some sort of public interest, like having reasonably priced spare parts and the right to a free information flow – the freedom of the press and freedom of speech. The international basis for this is article 17 of the TRIPs, which allows national exceptions for fair use.

4.1 About brands in the gaming industry

The computer gaming industry is highly *co-branded,* a term that means that several brands are used in conjunction with each other when communicating with the customers. Typically, the brand names of the companies creating and publishing the game are used together with the game brand. As I wrote in Chapter 2.6, the two most important types of

[98] WIPO, P 184.
[99] Found here: http://oami.eu.int/en/mark/aspects/reg/reg4094.htm#0090

actors on the computer gaming market are the developers and the publishers. This gives us three main levels of brands used on a given game; if the publisher and the developer is not the same company (EA for example, a major publisher, also develops their own games). The first level, the game name, is the most recognizable among customers. The second level, the developer, is not as recognizable, although more initiated gamers usually knows which developer it is who has created the game. The least visible brand is that of the publisher, many gamers probably don't know which publisher who has released the game. The first level, the game name, is the main brand, and big titles (called triple A) are recognized by a majority of the gamers – the brand has great awareness, i.e. a high percentage of the target population recognizes the name. A great awareness of a brand naturally leads to increased exploitation of that name, and it can thus contain sub-levels that distinguish the first game from its expansions and sequels.

Brands in the gaming industry:

1. Main Brand Name - Game Name
   1a. Main Brand + Sequel Name
   1b. Main Brand + Expansion Pack Name
2. Developer
3. Publisher

A prime example of this chain of interconnected brands is the smash hit of WarCraft. It started out as a real time strategy game called WarCraft: Orcs and Humans in 1994, and is one of the most successful RTS-games to date. This naturally spawned sequels, expansion packs and spin-offs, which were titled WarCraft II: Tides of Darkness, WarCraft III: Reign of Chaos. A spin-off further exploiting the WarCraft brand is the MMORPG World of WarCraft. Applying the list above to the most recent sequel to the WarCraft brand as an example, the structure emerges[100];

1. Main Brand Name	WarCraft
1a. Main Brand + Sequel Name	WarCraft III: Reign of Chaos
1b. Main Brand + Expansion Pack Name	WarCraft III: the Frozen Throne
2. Developer	Blizzard Entertainment
3. Publisher	Vivendi Universal Games

[100] Information from Blizzard: http://www.blizzard.com/inblizz/profile.shtml.

(Blizzard is a division of VU Games).

Since the Game Name is the name which has most awareness amongst customers, that brand is the one that also takes the "major beatings" and loses most in brand value if the shit hits the fan. A bad game, i.e. a game that sells too badly, will in all likelihood never spawn sequels. Just like movies, there has to be some calculated profit in the release of a sequel. Consequently, good games (i.e. games that sell reasonably well) will of course have higher brand values – high awareness – and will spawn many sequels.

The negative effects of a bad game may bleed over to the developer, who might gain a reputation as a bad developer, which in turn will affect future game releases. The producer however, the one who takes the financial risks, are the least visible. Many gamers know that Blizzard makes WarCraft, but how many knows that VU games publish WarCraft? Not as many, I would think. This problem is about the same regarding cheats. If a game becomes known as a game that contains many cheaters without the developer taking action, that game will lose sales no matter how excellent the game might be otherwise. Furthermore, its sequels and expansion packs will be equally affected as gamer's reason that the brand is infested with cheats. This reputation may bleed over to the developer of the game unless action is taken. This is exactly what happened to Blizzard and the famous Diablo brand[101]. The first Diablo game was overrun with cheaters and gamers left the brand in droves. When Diablo II was released Blizzard was forced to deal with the problem, as they were rapidly gaining a reputation as a developer with cheat-infested games. The reputation from Diablo was bleeding over to its sequel, and was about to or had already bled over to the developer. Blizzard was forced to take action or keel over, well, at least face substantial losses in sales. With tough measures like "Blizzard Removes 400,000 More Battle.Net Accounts"[102] they have regained the initiative and now have a significantly better reputation for dealing with cheaters in their games.

[101] See Kuo, who chronicles the Diablo history of cheating.
http://shl.stanford.edu/Game_archive/StudentPapers/BySubject/A-I/C/Cheating/Kuo_Andy.pdf
[102] http://games.slashdot.org/article.pl?sid=03/10/01/0534202&tid=206&tid=210&tid=10

4.2 The structure of the spreading of cheats

Most cheaters can not create their own hacks. It takes at least some programming skill and knowledge of the structure of the game in question to program a working hack. The same goes for bug-exploiting, although anyone who knows how can easily exploit a bug, he must first know about it. It is not easy discovering all usable bugs on your own, and at best only a few are found. Therefore most gamers inclined to cheat visit special websites that offers downloadable hacks and information on how to exploit bugs that others have found. During the research for this paper I quickly found no less than six sites offering hacks, cheat-scripts and bug-information to a variety of games. At least four of these charged money for access to the material. One site even had a disclaimer in which they claimed that the customer paid "for the ability to post in the forums, not for the content, files and/or links" but by a strange coincidence, no material was available until the fee was paid. Said site also stated in the disclaimer that the trademarks belonged to each respective company, that they took no responsibility for people violating the code of conduct for the games[103] and that if copyrighted material existed on the site it was not placed there intentionally. Nevertheless, this did of course not stop them from using the trademarks, encouraging people to violate codes of conducts and (presumably – I did not pay the fee to check it out) posting material that may infringe copyrights. Cheat sites normally 'advertise' on their frontal web page by compiling a list of all games that they provide cheats to, and gives access to those who pay. (Sites that do not charge for cheats exist though.)

Cheats may be spread in other ways. Certainly cheats can be spread directly from individuals to individuals with the use of file sharing programs – peer-to-peer networks and chat clients like mIRC, ICQ and MSN all have the possibility to send and receive files. But an educated guess would be that most cheats are delivered via websites and affiliated message boards, since the cheat creator reaches the largest audience that way. Most cheaters are notoriously shy and will try to remain as anonymous as possible, and connecting to a website is more anonymous then e.g. giving out your MSN address.

[103] See Chapter 5 regarding contractual obligations for computer games. Many companies forbid cheating in their games via License Agreements and Terms of Use contracts. These sets of rules are sometimes referred to as Codes of Conduct.

4.3 Stopping the spread of cheats using trademarks

In order to keep the brand name clear of cheats, a sensible brand manager will try to avoid having the brand figuring on cheats and hacks sites. Any mention of the brand name in such circumstances can affect the brand negatively, as it will contribute to spreading cheats to the game in question – and also tell the community that cheats are readily available for the game. The basic rule for trademark is, as I wrote above, that the owner of a trademark can prevent others from using the mark *in the course of trade.* This is a criterion all states that have signed TRIPs are bound by, and is for example found in the European Unions trademark regulation[104]. The exact scope of the criteria is a case by case judgement. The European Court of Justice ruling Hölterhoff v Freiesleben[105], as an example, stated that an oral use of the mark for a descriptive purpose regarding quality of goods was allowed. Nevertheless, the starting point is that every use in the course of trade is forbidden without the permission of the marks owner.[106]

"In the course of trade" is a wide concept (note that in the US, the concept is called "in commerce"). A dictionary defines the word trade as "*Noun 1. the commercial exchange (buying and selling on domestic or international markets) of goods and services"*[107] So basically, all actions that includes, or is intended for, money changing hands can be defined as in the course of trade. Thus the sites that charge for access to cheats are doing that in the course of trade, as they provide goods (software hacks and scripts) and/or services (like listing known bugs and how to exploit them, with regular updates). The goods and services are probably in the same class as the game, being game-software (hacks) or otherwise closely related to the game (bug-lists). The Nice classification system provides the following under class 9[108]; *Computer Game Programs*, under which hacks and scripts certainly fall. Regarding the lists of exploitable bugs in games and under which category they will sort under, I am not sure. It is probably reasonable to assume that such lists fall under "…goods or services which are identical or similar to those in respect of which the trademark is registered" (Article 16 TRIPs). Noteworthy is that sites providing cheats for free does not infringe trademark rights, as they do not use brands in the course of trade.

---

[104] Article 9**,** COUNCIL REGULATION (EC) No 40/94 of 20 December 1993 on the Community trade mark. Found here: http://oami.eu.int/en/mark/aspects/reg/reg4094.htm#0090
[105] Judgment of the Court 14 May 2002, Case C-2/00. http://oami.eu.int/en/mark/aspects/pdf/JJ000002.pdf
[106] Koktvedgaard et. al. P 390.
[107] Wiktionary: http://en.wiktionary.org/wiki/Trade
[108] http://www.wipo.int/classifications/fulltext/nice8/enmn09.htm. Serial No. C0769 (note that the serial number is the English version).

The basic rule is then obvious; every unauthorized commercial use of a trademark is prima facie forbidden, and the cheat sites have committed a trademark infringement when advertising with the brands and capitalizing upon them by selling goods and services connected to the brands. Article 9 of the European Community Trademark Regulation states;

Article 9 (Council Regulation on the CTM)
1. A Community trade mark shall confer on the proprietor exclusive rights therein. The proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade:
(a) any sign which is identical with the Community trade mark in relation to goods or services which are identical with those for which the Community trade mark is registered.

It is not a requirement (at least not explicit) that the use is "as a trademark"[109], for it to be forbidden. The extent of allowed usages is not clear at all, however. UK Courts have declared that infringements are trade mark uses, not other uses, as that is seen as inherent "in the notion of using a sign in the course of trade"[110]. Cheat sites does not use any single game brand as trademark, rather they list a number of brands and declare that they provide cheats to those brands under their own trademark (- the name of the site most often). Thus no game brand is singled out and used as a *distinguishing feature* for the goods and services provided on the cheat sites. The use is descriptive, merely detailing what brands they provide goods and services for.

This is in the US called *Nominative fair use* which states, that if a user can show the following bullets the use should be regarded as fair, if he is only using the trademark to describe the product the trademark covers[111] (a form of descriptive use);

- First, the product or service in question must be one not readily identifiable without use of the trademark.

You can hardly sell cheats without telling your customers which game they are to be used for. Compare with selling spare parts or other types of add-on products.

[109] Cornish et al. P 702.
[110] Ibid. P702.
[111] This principle of nominative fair use is for example outlined in the case; The NEW KIDS ON THE BLOCK et. al. v. NEWS AMERICA PUBLISHING, INC. et. al. v. GANNETT SATELLITE INFORMATION NETWORK, INC., d/b/a/ USA Today, Inc., Nos. 90-56219, 90-56258.
United States Court of Appeals, Ninth Circuit, from which the bullets are quoted. Found here:
http://cyber.law.harvard.edu/metaschool/fisher/integrity/Links/Cases/newkids.html

- Second, only so much of the mark or marks may be used as is reasonably necessary to identify the product or service.

The cheat sites rarely or never (I have not seen it) use the logos, or the any other parts of a trademark beyond the words of the mark.

- Third, the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder.

The cheat sites do not indicate that the cheat is officially sanctioned, rather the opposite is true.

The rebuttal to this is that fair uses or uses in good faith are usually exceptions designed to protect some sort of public interest. What public interest is protected when allowing people to make money on actions that destroys the reputation of brands? The media may from time to time do exactly that, for example publishing sometimes dubious reports that certain brands of cars are death-traps, of bad quality or the like, and as a consequence selling tons of copies or getting higher ratings. But they also act in the interest of the public – the right to know, the freedom of press - since if the media happens to be right it is extremely vital that information is not covered up. Selling cheats does not fall under any such category; it is hardly a human right to cheat in computer games. To sum this line of reasoning up, it is fairly uncertain if the pay-for-cheat sites use of game brands can be seen as an infringement. If seen from the perspective that advertising (by listing games they provide cheats to on the main page) and using the brands results in lower brand values for no legitimate reason the basic principle is that every commercial use is forbidden, a court may very well find it to be an infringement. If seen from the perspective of nominative fair use, and that the brand is not used as a distinguishing feature as a trademark and taking into account that the risk for confusion is low, it should be allowed.

A few words should also be said about the protection for well-known marks, which is significantly broader than for ‘ordinary’ marks. Consider Article 9 of the Council Regulation;

Article 9 (Council Regulation on the CTM)

(c) any sign which is identical with or similar to the Community trade mark in relation to goods or services which are not similar to those for which the Community trade mark is registered, where the latter has a reputation in the Community and where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the Community trade mark.

Or the US Trademark Act;

§43 (15 U.S.C. §1125). False designations of origin; false description or representation
(c) (1) The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection.

If the owner of the mark can prove that the brand has a reputation or is famous[112], his protection will increase. These provisions started out as aiming for an anti-dilution effect, but the wording has been expanded by case law both in Europe and in the US. Not only can the owner prevent uses of the brand for classes of goods and services for which the mark is not registered or used, he can also prevent the reputation of the mark when used in circumstances deemed detrimental (such protection has been advanced by case law and derogates slightly from the wordings of the law[113]). The use of the trademark on cheat sites can be said to be detrimental to the reputation of the brand, and it may thus be an infringement. It may even be possible to sidestep the demand of "in the course of trade" as long as the detrimental effect is economical.

4.4 Responsibility of Online Service Providers regarding Hacks – the US

The definition of an online service provider is quite broad; the US Copyright Act defines it as[114];

US Copyright Act, Article 512 (k)
1) Service provider. - (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

[112] The process for this can be long and complicated, but a large awareness amongst the target clientele for the product is usually enough. In gaming circles, this would probably include many AAA titles – such as the WarCraft brand, Counter Strike and so on.
[113] McCarthy, http://www.inta.org/downloads/tmr_McCarthy.pdf
[114] Found here: http://www.copyright.gov/title17/92chap5.html

Basically, an Online Service Provider (OSP) is an entity that provides services online, which includes Internet Service Providers (ISPs, the ones who facilitate the actual connection to the Internet. Note that some ISP provides server space for websites in their services). The term thus includes companies who sell server space, e.g. for a website. The 512 Section was included with the Digital Millennium Copyright Act, and is generally referred to as the "DMCA takedown provisions". The section outlines a set of rules the OSPs must adhere to if they wish to avoid liability for copyright infringements conducted by their users, 512 is thus as set of limitations on liability. Otherwise an OSP might be found guilty of third party liability - specifically contributory or vicarious liability.

Section 512 (c) relates to cases concerning OSPs who operate servers for websites and message boards (and a host of other different situations, but the two mentioned are the most interesting regarding the spread of hacks) as it applies to storage as directed by the users. It states that[115];

US Copyright Act, Article 512 (c)

c) Information Residing on Systems or Networks at Direction of Users. -
(1) In general. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -
(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

One can conclude that an OSP might be liable for monetary relief if he does not comply with these provisions, which gives him a strong incentive to investigate any claims sent by the infringed party as soon as possible and act accordingly. The provisions is such that

[115] Found at; http://www.copyright.gov/title17/92chap5.html

some think it is misused to "silence other users", since some OPS's seems to respond to any cease and desist letter by simply taking down the material without investigating the matter[116]. Important to note is that the DMCA takedown provisions are strictly regarding copyright infringements, not trademark violations or other issues one might feel should be taken down. The DMCA 512 also lists a set of formal requirements that needs to be met. E.g. the OSP must have a service agent that receives the claims, and the claims must adhere to standards of proper notification. These issues are often overlooked or ignored[117], which may in time lead to a less effective provision.

The US Copyright Act and the 512 are of course only valid in the United States, for infringements conducted in the US. Nevertheless, companies outside the US might follow its provisions anyway if they have any significant business in the US and wish to avoid a lawsuit. In any case the bottom line is that if hacks are regarded as copyright infringements (see Chapter 3.4-5 above for that discussion), the infringed party can, under the 512 DMCA takedown provisions, demand that the OSP removes the infringing material and in that way limit the spread of hacks.

4.5 Responsibility of Online Service Providers regarding Hacks – the European Union

The situation in Europe is somewhat different. No supranational legislation corresponding exactly with the takedown provisions in the US can be found in the European Union as of yet. It is possible that individual member states have enacted some sort of similar provision, but it is far beyond the scope of this paper to investigate the legislation in all the 25 member countries (when this is written, currently 4 states have candidate status)[118]. Nevertheless, as I wrote above, some companies comply with the DMCA even if it is not valid in the EU, out of fear that an American judge will seize assets the company may have over there (consider, for example, a large service provider with its base in the US but with a large number of customers in Europe, or the other way around). However, the same sort of principles regarding the responsibility of OSP's can be found in the EU as in the US. The "Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions" from 1999 states that "*The online service operator generally assumes editorial responsibility*

[116] For example, see http://chillingeffects.org/, from which the quote was taken, off the front page.
[117] See the lists of notices at http://www.chillingeffects.org/copyright/notice.cgi
[118] http://europa.eu.int/abc/index_en.htm#

for such content, like a traditional publisher."[119] OSP's might thus find themselves liable for infringement according to third party liability principles, for illegal material posted on their servers.

The e-commerce directive[120] is probably the closest thing the European Union has to the DMCA, and it aims, among other things, at implementing takedown provisions in the European Union similar to the DMCA.[121] It concerns not only copyrighted material, but all storage of information on web-pages. In that aspect the e-commerce directive is wider in its scope than the DMCA, since it can also be used to attack other illegal usages, such as trademark infringements. It does not, however, have the rigid rules of proper notice and such, but is more a framework of principles the member states are required to implement in their national legislation. The exact definitions of "Online Service Provider" and the context in which the legislation is valid also differ somewhat, but for the purposes of this paper they are the same. Article 14 details the aspect of hosting illegal material;

Article 14 *(The e-commerce directive)*
Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an

119 Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. http://europa.eu.int/ISPO/legal/en/internet/communic.html. Editorial responsibility is a term taken from the newspaper context, it means that the editor is legally responsible for all that is published in the paper and could find himself sued for slander, Intellectual Property infringements etc – for something he did not actually write himself.
120 "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')" Found here:
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML
121 Cornish et al. P 800.

infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

When combined with Article 15, which states that service providers does not have a general obligation to monitor information they transmit or store, it becomes clear that the system is primarily built upon notice. The provider is exempt from any liability if he acts expeditiously to remove illegal material upon request, or if he does not know about it. Since he do not have an obligation to monitor content, it is almost certainly so that he must be notified to have any sort of responsibility, especially regarding such grey areas as copyright infringements regarding hacks to multiplayer online games, and other such IP violations. Similar to the situation in the US under the takedown provisions, companies may use the strategy of notifying OSP´s that they host illegal copyrighted material (e.g. in order to limit the spread of hacks). This has led to much of the same critique as the DMCA takedown provisions has faced in the US, when countries ponders how to implement the Directive in Europe. Some claims that a private censorship is inherent in article 14 of the Directive, since OSP's now must decide what constitutes illegal information on the basis of the allegedly infringed party and remove it, or otherwise risk damage claims.[122] In what direction these takedown provisions take us remains to be seen, but given the anonymous and illusive nature of cheat-creators, getting to them via their OSP's might be the one of the few viable ways to stop the spreading of hacks.

[122] Marzouki, http://www.edri.org/edrigram/number2/france

Chapter 5: Contractual Obligations and stopping the use of Cheats

Software is almost always sold and/or distributed[123] as a license, which means that what you buy is not really the actual DVD or CD disc, but rather a right to use the included software. You of course own your computer and the disc, but the final ownership of the copyrighted material still belongs to the company that sold you the license. This is perhaps even clearer when the software is downloaded directly to the user's computer; the user does not own the downloaded files in any sense of the word – but gains a right to use them under certain conditions. The license agreement is called End User License Agreement (EULA) and contains certain conditions, often restricting the user in various ways. The benefits of using a license instead if letting the law cover the agreement[124] is that the companies can include clauses that limit their liability, try to prevent reverse engineering contractually, disclaim any warranties, forbid the user to rent the software out, limit the amount of computers the software may be installed into and basically everything else they think is important[125]. EULAs that comes with computer games frequently include sections forbidding the use and creation of cheats, and sometimes clauses preventing bug exploiting and other types of undesirable behaviour, thus establishing a contractual Code of Conduct for the playing of the game (Codes of Conduct are especially common in MMORPG's).

These EULAs are standard contracts that apply to every customer of the product, and the benefits are obvious. Negotiating terms with every individual interested in the software is not only nigh on impossible, it is also incredibly inefficient[126]. Significantly lower transaction costs can be achieved with standard contracts for every customer with "take it or leave it" provisions. That which is so special regarding software EULAs is that they are frequently entirely digital in nature. The agreement is distributed and accepted exclusively in electronic form. Analogue agreements in the form of contracts are

[123] "Free" software, like patches and extra maps to games, are not sold per se but distributed freely. Nevertheless, they are subject to license agreements as well.
[124] Some laws are non-mandatory, meaning that an agreement between the parties supersedes the law. Mandatory laws though, are written to protect some interest deemed important enough, thereby giving customers rights that are non-negotiable. For example, the right to reverse engineer software is mandatory in Sweden. This according to 26 § g of the Swedish Copyright Act, the same text as in article 5(3) of Directive 91/250/EEC. http://europa.eu.int/ISPO/legal/en/ipr/software/software.html
[125] DiMatteo, P 401.
126 Grossman, et al.. http://www.becker-poliakoff.com/publications/article_archive/click_wrap.htm

physically signed, whereas wrap-agreements are either just a unilateral statement from the licensor to which the customer implicitly agrees, or a unilateral set of terms that the user accepts explicitly with the click of a button. These digital EULA's come, regarding software, in two shapes;

- Shrink-wraps, so called because the customer is bound by the license agreement when he tears the plastic in which the box containing the software is placed. The terms of the agreement are then usually found included in the software – or placed in paper form bundled in the box. A text on the box states that tearing the plastic subjects the customer to the agreement. Shrink-wraps are thus based on implicit agreement by the customer, as he is deemed to agree by the terms when he tears the plastic.
- Click-wraps, (also called click-throughs) when the software is about to be installed a box containing the agreement pops up, and the user is required to click "I agree" or something like that, before the installation can proceed. There are two basic designs for click-wraps; one is called "type-and-click", when the customer is required to type "I agree" and then click a send-button, the other is "Icon-click" when the customer clicks an icon stating "I agree".[127] Click-wraps are used for software directly downloaded from the Internet, but also in lieu of shrink-wraps for software bought in stores. Click-wraps are based on explicit agreement by the customer, as he takes explicit action when confirming his acceptance by a click.

A third form of the wrap agreements is worth mentioning;

- Web-wraps (or Browse-wraps), are a link located on webpage stating that the individual is bound by the agreement which can be read if the linked is followed.[128] The agreement resembles an EULA rather closely, but is called Terms of Use, Terms of Service or Terms of Agreement depending on type of agreement. Note that the terminology is nowhere near unified though, for example, EULAs are sometimes called Terms of Use instead. Nevertheless the intention of licensor is clear – to govern the relationship with the licensee. Like shrink-wraps, web-wraps are based upon implicit agreement. Merely surfing a web-site with a web-wrap notice on it may bind you to the company's Terms of Use.

[127] Grossman, et al. http://www.becker-poliakoff.com/publications/article_archive/click_wrap.htm
[128] Darden et al. http://gsulaw.gsu.edu/lawand/papers/su03/darden_thorpe/#II

As I mentioned above, gaming companies usually include anti-cheating clauses for their software licenses and for their user-licences on their web pages (e.g. Blizzards battle.net). I will discuss the validity of these agreements, first generally regarding enforceability of wrap agreements, and then analyze anti-cheating clauses specifically.

5.1 Enforceability of wrap agreements – US

There has been much debate, and there still is, regarding the validity of wraps-agreements in the legal world. The underlying principle for contract law is *"pacta sunt servanda"* – agreements shall be kept, which is a rather self-evident rule. If people could avoid obligations they had agreed to, society would descend into chaos rather quickly. Nevertheless, the rule has several exceptions. First, it must be established that an agreement has been reached. Other exceptions handle the person who agrees to the contract; minors for instance, can not be legally bound by their word. Another important exception is regarding consumer customers; many countries have in their legislation (and/or in court judgements) recognized the vast differences in bargaining power between a large corporation and a consumer and have therefore taken steps to ensure that consumers are not bound by unfair and unreasonable terms. The intricacies of contract law can thus extend far beyond the simple maxim, and the unilateral EULAs must not necessarily bind a customer.

Three main problems have arisen regarding wrap-agreements, mainly in the US from where the majority of court cases hail. They are *notice, consent* and *fairness*.[129] (Refer to this article (linked in note seven) for an extensive review of the US case law regarding *click-wraps* and *web-wraps* with links to court cases, below you will find a brief summary sufficient for the purpose of this paper.)

- Notice

Rather obvious is the fact that if someone is to be bound by an agreement, he must *know* he is. This is generally not a problem regarding click-wraps, as a window pops up and notifies the user. Shrink-wraps frequently have notices on the outside of the box, proclaiming for the customer that a license agreement comes with the purchase. Web-wraps, however, can be close to invisibly placed – enforcing such web-wraps will be problematic.

[129] Darden et al. http://gsulaw.gsu.edu/lawand/papers/su03/darden_thorpe/#II

In the famous case ProCD v. Zeidenberg[130] the court enforced a shrink-wrap license, and stated that displaying the entire license agreement on the box was not feasible. Sufficient notice was given if a label was placed on the box referring to the license agreement. The court held that shrink-wraps were generally enforceable if they fulfilled three criterions: 1) Notice on the box stating that the purchase was subject to a license agreement. 2) The license agreement available in the box and 3) the buyer should have the right to return the merchandise and get a refund if he did not agree to the terms. The courts reasoning was in part that invalidating the widespread use of shrink-wraps would lead to higher transaction costs for the companies, which in turn would lead to higher retail prices and thus make consumers worse off. The court also stated, regarding the digital context, that "transactions in which the exchange of money precedes the communication of detailed terms are common", meaning that consumers buying other types of goods in the analogue world, often do not know the terms of the purchase before the buy.

Click-wrap agreements have been deemed by US courts as giving sufficient notice in the pop-up box as to the existence of a license agreement. In Forrest v. Verizon Communications[131] the court said "one who signs a contract is bound by a contract which he has an opportunity to read whether he does so or not." Web-wraps have been found giving sufficient notice on the grounds that the existence of a license agreement or Terms of Use was advertised on the web-pages[132].

- Consent

For a binding contract the contracting parties must have mutually assented to the terms. Analogue contracts accomplish this with the signing of the contract, or a simple oral assent – a "yes". Click-wraps, again, accomplish this rather easily with the explicit "I agree" button, but do not take into account mistakes or accidents (theoretically one could claim that a slip of a finger or a mischievous cat agreed). Shrink-wraps and web-wraps relies on an implicit assent, the tearing of plastic and surfing the page, which has led to problems when enforcing these types of contracts.

[130] ProCD v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996). Found here: http://digital-law-online.info/cases/39PQ2D1161.htm
[131] Forrest v. Verizon Communications, Inc., 805 A.2d 1007 (D.C. 2002).
[132] In Pollstar v. Gigmania Ltd., 170 F.Supp.2d 974, (E.D. Cal. 2000), and Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238, (S.D.N.Y. 2000).

Regarding shrink-wraps and consent, the court found a shrink-wrap agreement enforceable in Hill v. Gateway 2000, Inc.[133]. The licensee received a computer (this case is especially interesting because it was not about software) and the agreement. The contract stated that if the licensee kept and used the merchandise for more than 30 days, they agreed to the terms of the contract. Moore v. Microsoft Corp[134] held the Microsoft's click-wrap EULA was valid, since the license agreement was prominently placed on the screen, and the user was required to click an "I Agree" button before proceeding. In contrast, two web-wraps were held unenforceable[135] since the prospective licensee had not given consent to the agreement.

- Fairness

This problem is in no way unique to wrap-agreements. As I mentioned above, differences in bargaining power leading to unfair terms can result in clauses and entire agreements being declared invalid in court, but this problem is the same in any situation where a company deals with a consumer. What is unique to the wrap-context is that no personal contact is involved, e.g. salespersons that can discuss and explain the terms should a question arise. Furthermore, the "dust" has not settled yet. Wrap-agreements are relatively new, and the software industry, the legislator and the courts have yet to reach the balanced agreements found in other industries that use unilateral contracts against consumers. One common critique against EULAs is that they sometimes resemble more of a wish-list from the licensor, rather than a legitimate contract.[136]

A wrap agreement regarding fairness was Comb v. PayPal, Inc.[137], which found the entire agreement invalid because of its long, hefty and onerous provisions against consumers, particularly an arbitration clause calling for proceedings significantly more expensive than other available options.[138]

---

[133] Hill v. Gateway 2000, Inc. 105 F.3d 1147 (7th Cir. 1997).
[134] Moore v. Microsoft Corp, 293 A.D.2d 587, 741 N.Y.S.2d 91 (N.Y.A.D. 2 Dept. 2002)
[135] In Specht v. Netscape Communications, 306 F.3d 17 (2d Cir. 2002), and Ticketmaster Corp. v. Tickets.Com, Inc. 54 U.S.P.Q.2d 1344, 2000 WL 525390, 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000).
[136] See for example page 5 of Rolston.*
http://www.avault.com/articles/getarticle.asp?name=eulapt1&page=5
[137] Comb v. PayPal, Inc., 218 F.Supp.2d 1165 (N.D.Cal. 2002).
[138] Arbitration clauses against consumers are generally frowned upon. Arbitration is a "private" court in which the parties choose the judges according to the rules of different arbitration institutes. Although arbitration is faster and low-profile compared to courts (court judgements are public, arbitration judgements are secret), the costs are significantly higher in most cases. The Swedish law, for example, forbids the use of pre-conflict arbitration clauses against consumers ("Lag (1999:116) om skiljeförfarande", section 6), such clauses are invalid.

An attempt to codify the issues regarding wrap-agreements in the US was made in the Uniform Computer Information Transactions Act (UCITA)[139]. It has, to date, been largely unsuccessful, since its enactment has been limited. It appears to have a strong bias towards licensors, and many consumer groups have attacked it.[140] Proponents of the UCITA hold among other things that it merely codifies existing case law regarding validity of wrap-agreements, and that it creates statutory rights for the invalidity of unconscionable terms.[141] Time will tell if UCITA will be the definite authority on the area, as states in the US discuss whether to enact it or not.

In conclusion, the wrap agreements are generally valid as license agreements in the US, with a disclaimer for web-wraps. A small, or otherwise hard to notice, web-wrap notification may not be sufficient to legally bind anyone – particularly since the prospective licensee does not have the opportunity to consent to or reject the terms.

5.2 Enforceability of wrap agreements – Europe

The widespread use of wrap-agreements in the industry has basically led to a world wide standard, an industry practice.[142] Virtually all software sold or released everywhere in the world are subject to EULAs in click-wraps or shrink-wraps. Therefore it is more a question of time until wrap-agreements are recognized everywhere, but as of today many jurisdictions are trying to tackle the question.[143] Particularly as some judgements in US courts seems, with for example Swedish eyes, quite harsh against consumers,[144] although this critique is also focused on the content of the agreements, rather than merely on how they are entered into. Regarding contract law, it should be said that no legislation from the European Union have harmonized it. Every state has its own tradition and legislation, and although similarities can be found[145], there are also substantive differences. This makes it harder to produce a single conclusion for the European Union regarding wrap-agreements. It may be so that one country finds a certain wrap-agreement enforceable, whereas another denies similar agreements enforceability.

---

[139] Found here: http://www.law.upenn.edu/bll/ulc/ucita/ucita1200.htm
[140] http://www.faqs.org/docs/ecom/transactionstext.html
[141] Grossman, et al. http://www.becker-poliakoff.com/publications/article_archive/click_wrap.htm
[142] Robertson. http://elj.warwick.ac.uk/jilt/cases/98_2rob/dwnloadf.htm
[143] Collins, http://www.design-ireland.net/index.php?http%3A//www.design-ireland.net/e-commerce/business-12.php
[144] Pawlo, P 150.
[145] The Nordic countries, for example, share many traits with each other.

There are very few court cases in Europe regarding wrap-agreements, but the Scottish court case Beta Computers v. Adobe Systems[146] is an example. The court held that shrink-wraps are generally enforceable; although in this particular case the customer won (the question was if the customer could return the software unopened, but the court recognized the validity of shrink-wraps per se). It was stressed in the judgement that it was "dictated by the particular facts of the present case" (this is a common disclaimer when courts wish to avoid placing too much significance on a case), the fact that the order was placed over the phone meant that discussion regarding terms of the license could not take place until the software had been received, which in turn meant that the final completion of the contract is *not* the delivery of goods,[147] but the implicit (or explicit) agreement to the terms of the license.

Regarding electronic contracts in general, an interesting article can be found in the e-Commerce Directive[148];

Article 9 *(E-Commerce Directive)*
Treatment of contracts
1. Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.[149]

This is a rather non-committal article regarding click and web-wrap-agreements (shrink-wraps are not concluded electronically). What it says, basically, is that electronic contracts should be treated like "normal" contracts. It does not address the specific problems arising from wrap-agreements, like if sufficient notice is given when software is bought, i.e. that it is subject to a click-wrap license agreement that needs to be accepted before installing can proceed. Nevertheless, should anyone decline the license agreement, it is very likely that similar to established practise in the US regarding shrink-wraps (see

[146] Beta Computers (Europe) LTD v Adobe Systems (Europe) LTD Outer House, 1996 SLT 604, 1996 SCLR 587.
[147] Lloyd, http://europa.eu.int/ISPO/legal/en/tourtabl/lloyd.html
[148] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML
[149] Exceptions from this article can be made in cases where the contract is not valid unless certain formalities are fulfilled, e.g. a witnessed, signed contract drawn up in a special way, according to paragraph 2 of the article. The sell of real estate is an example.

ProCD v. Zeidenberg), a right to return the software and get a refund exists. There are problems regarding software return and refund though. "Normal" goods can be returned without any problems, there is no way the average consumer can copy a toaster, for instance, and then return it. But software can be copied, albeit with some effort[150], thus the consumer can theoretically both have the cake and eat it (this is a rather theoretical problem however, as it is even easier for the customer to download the program from a file-sharing network and use it). Furthermore, many computer games come with a unique CD-key that gives the consumer a unique identity online. This CD-key is checked for validity against a special centralized server in multiplayer games, allowing the player to play online, whereas an invalid CD-key only allows play offline.[151] Therefore the CD-key comprises a major part of the purchase, and returning games with the CD-key compromised is highly dubious (only one unique CD-key can be in use at any one time). Compare with used underwear, they drop dramatically in value once bought and opened, and are therefore never refundable. Computer games with multiplayer capacities are, for those who intend to play online, worth next to nothing if the CD-key is leaked. It is, of course, not legal to play with a CD-key the user is not entitled to, as the game is pirated. Nevertheless, the CD-key system poses a problem to the decline of EULAs and the subsequent return and refund of the game, as the store will be unable to sell the opened game (or at least have to deal with angry customers whose CD-keys are leaked).

There is a point to writing articles so general in scope however; the development of the Internet and its related businesses is fast. Specific legislation has in some cases proved too slow – i.e. being obsolete even before its released – old technology being replaced with new thus changing the circumstances. Nonetheless, the ambiguity and vagueness of the Directive have drawn critique, among other things that the unclear directive may lead to different implementations in national law.[152]

What *can* be inferred from the article, in my opinion, is that *click-wraps* per se should be enforceable in the European Union. Non-negotiable standard contracts are used in business-to-consumer (B2C) and business-to-business (B2B) transactions regularly; the only major difference is that click-wraps are concluded electronically. Similar arguments

[150] It should be noted that circumventing copy protection for no legitimate reason is illegal both in Europe and the US, according to article 6 of Directive 2001/29/EC and § 1201 of the US Copyright Act.
[151] "Cracked" games comes with a CD-key generator, which delivers CD-keys that can be used to unlock the game when it is installing, but these cracked CD-keys are not valid for online play unless the server is cracked as well.
[152] Ramberg.

can be put forward to support the validity of shrink-wraps. For example, did you read the contract you entered into the last time you rented a video or DVD film? Those are available in paper form, and you actually sign a slip. The fact that the licensees commonly do not read the contract is sometimes used as an argument against wrap-agreements is not a valid one seen from that perspective. Web-wraps are another issue entirely though, it is my belief that actually enforcing web-wraps will be difficult. Like highlighted in the court cases from US above, it is next to impossible to show that someone has noticed that their actions are subject to a web-wrap. It stands to reason that binding someone legally with a contract without him having a clue about it is out of the question.

Two American lawyers wrote this analysis regarding international enforceability of wrap-agreements in 2000[153]; (Quote is cut to only include European Union countries and Norway)

"Based on the advice of local counsel, we believe that traditional shrink-wrap agreements are likely to be enforced in countries including ...France, Italy, Spain, Netherlands, Denmark, Norway, Sweden, Finland... Enforceability is ...unlikely in Germany, the United Kingdom.

Click-wrap agreements, however, may be a different matter. Click-wrap licenses may actually be easier to enforce in most of the above countries because the licensee can review the terms and conditions before accepting and affirmatively manifesting his or her acceptance of such terms and conditions."

I agree with their analysis (except shrink-wraps in the U.K – English law may yet declare that they are unenforceable, but the Scottish case referred to above seems to indicate that shrink-wraps are enforceable at least in Scotland) that click-wraps should be enforceable in the EU, an opinion, which in my view, is further augmented by article 9 in the e-Commerce Directive. A problem regarding computer games and wrap-agreements that needs to be solved is the question of CD-keys and refund should the terms be unacceptable for some reason – though the problem may be moot since people seems to accept the terms without actually reading them.

The question regarding the *contents* of the wrap-agreements is a different one. The software industry seems to have a tradition of drafting B2C clauses that can be far-reaching and outright ridiculous in effect. It is an educated guess that most European

[153] Contreras, et al. http://www.wilmerhale.com/publications/whPubsDetail.aspx?id=1c693d50-4976-4339-989a-bff98bb48730

courts will declare onerous B2C provisions void to a greater extent than perhaps an American court would. Directive 93/13/EEC[154] provides, among other things, a unified legislation concerning the invalidity of pre-formulated standard contracts with unfair terms against consumers. For example, the US case Caspi v. Microsoft Network[155] was regarding a click-wrap which had a forum selection clause in Microsoft's favour (licensees wishing to sue Microsoft had to do it in Washington, irregardless of domicile). At least in Sweden consumers have the mandatory right to sue a company in the court closest to where they live, and I am quite certain similar rules are found in most countries in Europe.

As a general conclusion, wrap agreements (click and shrink) are probably enforceable in the EU and US generally as valid contracts, whereas it depends of the content of the agreement if the courts will uphold the license and specific clauses of it.

5.3 Maximizing enforceability

If wrap agreements are to function effectively as means to prevent cheating in games it is of course important that they are enforceable. Should a court find a EULA unenforceable, it may create a dangerous precedent regarding contractual obligations in computer games. The point is that if courts start declaring clauses and even entire EULAs invalid, chances are that they will lose their legitimacy and subsequently be ignored - the instrument will lose its ability to influence customers in the desired way. What seems especially important is to adapt the EULAs to international circumstances, e.g. as clauses adapted to American conditions may be frowned upon in Europe. I have clicked through numerous American EULAs myself, quite convinced that should I initiate a conflict with company X, I will not be forced to travel around half the world to partake in the proceedings. Neither do I believe that in the unlikely event a computer game because of some extremely bad written code cause my brand new 500 € TFT screen to crash and burn (figuratively speaking) my claim is limited to nothing(!) or some 50 € .

Many guides have been published regarding strategies to maximize the enforceability of EULAs (content) in wrap-agreements, and wrap-agreements in general (the actual way

[154] "Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts". http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:EN:HTML
[155] Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. App. Div. 1999).

these contracts are entered into).[156] I shall not list every advice I have found, but rather focus on a few bullets I believe are particularly important in the computer gaming context.

- International Adaptation[157]

The company who intends to sell games outside their own country should be aware that no single version of the EULA can be expected to hold up around the world. Actions that needs to be taken on the key markets includes translation to domestic languages, since you can not expect anyone to be bound by something he do not actually fully understand. Although English is close to universal as a language, particularly in the gaming community, understanding complex legal provisions can be hard enough in your own language and thus even harder in your second language. Furthermore, local counsel should be contacted to review the EULA and adapt it to national circumstances. A clause that comes off as particularly unreasonable under that country's law should of course be removed and provisions that may cause the entire agreement to be void is a given no-no. The costs for this need not be as large, compared to the entire budget of an AAA title, translation and adaptation of the EULA is not a significant expense if done for the key markets. (For example, this would in Europe probably include Germany, France, Italy, Spain, the Benelux countries and the Nordic countries, and to some extent the UK.)

- Draft clear, concise and understandable contracts

Lawyers tend to speak "legalese"[158], a special technical terminology with long sentences and carefully phrased wordings rarely seen in any other context. The intention is to reduce the chance of unintended interpretations, but an unfortunate side effect of this is that normal people with no legal background find it hard to understand legal documents. This is a problem in EULAs targeted at a consumer audience. Other companies probably have their own lawyers who speak legalese, but consumers have only themselves. If they encounter long, boring documents packed with legalese, chances are they will ignore it. It is therefore better to make an effort and produce understandable contracts, which will increase the chances of people reading, understanding and actually adhering to the contracts. This is especially true regarding gamers, I think. When you have a new game, you really only want to get on with playing it as fast as you can, not sift through endless paragraphs of legal mumbo-jumbo.

[156] Here is one short and to the point; http://www.fenwick.com/docstore/publications/Corporate/Top_10.pdf
[157] Contreras, et al. http://www.wilmerhale.com/publications/whPubsDetail.aspx?id=1c693d50-4976-4339-989a-bff98bb48730
[158] In its most extreme form, legalese is packed with latin sentences.

- Availability

The EULA should be easy to find. It should not be a "one-time" event for the consumer (like when the click-wrap pops out during the installation), because chances are that the player will click his way through it and then forget about it. Instead the EULA should be posted on the games website under a special heading – so that it can be read before the purchase, it should be referred to every time the game is started and it should be easily found in connection with the game (e.g. a shortcut in the games folder under the Windows start menu, in the game's in-game menu and so on). It should be possible to save the EULA when it pops up with a single click, and a print-option ought to be included. The more the player is confronted with the EULA, the higher the likelihood of a court enforcing it and the higher chance of a player actually reading and adhering to it.

- Draw attention to important clauses

There are many ways to highlight important clauses with the technical means available on computers. Different colours, larger font sizes, bold or italic letters, requiring individual clauses to be checked with a dedicated "I agree" box next to them, playing a sound when the clause is reached with the scrollbar and so on[159] - they can and should be interactively and pedagogically presented, not hidden away at the bottom of the window. My point is that clearly stating for the user that cheating in this game is a breach of contract can only have benefits. Like the availability bullet above, it is important to show that there is nothing to hide.

- Contracts with minors are unenforceable

EULAs that comes with games probably run a much higher risk than many other agreements to be accepted by a minor (also keep in mind that the age may vary, most countries allows people 18 years old to enter into contracts i.e. the age of majority is reached at 18, but the span can be between 16-21). For example, 30 % of the most frequent computer game players are under 18 years old.[160] But also note that 97 % of those who buy computer games are 18 years or older.[161] One can surmise that a large portion of those buyers actually purchase for their kids. Anyhow, this means that a

[159] On a side note, I would like to say that the practise of writing important clauses in capital letters is an abomination. Not only do the caps make it harder to actually read the important clause, sometimes they annoy me so much that I actually tend to skip them.
[160] http://www.theesa.com/pressroom.html (Found under the "Demographic Information" tab, checked in February 2005.)
[161] Ibid. Note that these figures are from the US and their validity for Europe is uncertain.

significant portion of the gamers is not bound by the EULA, as they can not legally agree to it. To increase the chances of enforcing the EULA, the minor's parents should be involved and grant the minor permission to agree to the license. For example, the parents can be notified with a text on the outside of the box, the minor can be asked to fetch them during the installation of the game, or the clerks in the stores can be asked to notify buyers of the fact that license conditions are included and that they need to agree for any minors playing the game. Nevertheless, this is a problem that in the foreseeable future can not be worked around reliably. It is rather hard, should the need arise, to prove in a court of law who actually agreed to a wrap EULA. Although reasonable measures like the ones I listed above can decrease the risk of minors agreeing. Until a reliable implementation of individual electronic signatures is completed (a matter of time, I believe) so you can be a hundred percent sure about who actually agreed to the license, this is a risk that the gaming companies have to include in their calculations in the fight against cheats.

5.4 Stopping the use of cheats with software

The prevailing method of fighting against cheats (hacks and scripts) is via the use of monitor software, some sort of program that scans the player's computer for forbidden files, altered values and such. A prime example of this technique is Even Balance Inc. and their product PunkBuster[162], a company that provides an anti-cheating tool for a fee from the game developer or publisher. PunkBuster is, when this is written, exclusively used for FPS-games. Valve provides their own anti-cheat program called Valve Anti Cheat (VAC) for Counter Strike. MMORPG's does not normally use third party software, instead relying on the efforts of the supporting staff.[163] Blizzard, the developers of the popular RTS-games WarCraft and StarCraft also handles their anti-cheating efforts themselves, primarily via updates in the form patches and account monitoring on Battle.Net.

In addition to this, you can also find private anti-cheat initiatives, i.e. programs made by users that have tired on cheats and write their own programs to combat them. An example of this type of community effort is United Admins[164] – a non-profit organization funded with sponsorships and donations. Similar organizations, albeit not so organized, have

[162] http://www.punkbuster.com
[163] MMORPG's collect monthly fees from their users, and can thus afford to have a permanent staff monitoring the game.
[164] http://www.unitedadmins.com

grown around PunkBuster. PunksBusted[165], for example, is a private non-profit organization built around PunkBuster – they do not have their own anti-cheat program. What they do is collect information from servers running PunkBuster and maintain a *master ban list* (MBL) of people caught cheating. Server admins can even connect their servers automatically to PunksBusted servers and stream live information. What this means is that if a cheater is caught on one server belonging to the MBL, he is banned (blocked from entering) on all MBL-servers.

In the online gaming world, few are more despised or hated than a cheater. Therefore cheaters tend to anonymity, which is fairly easy on the Internet and the online gaming world. The name other players see on the server can be changed with a simple command, IP-addresses can be changed and faked, new accounts can be set up and so on. Anti-cheating efforts focus on eliminating that anonymity, so that caught cheaters can be identified and banned. MMORPG's use permanent accounts that the player's pay for, Battle.Net have similar accounts. PunkBusted use the CD-key to assign a unique ID number that the player is recognized by. It is of course possible to change CD-key, if a new one is obtained, and thereby the identity. Therefore PunkBuster have developed a system that identifies components in the computer – meaning that new computer parts are needed to change the identity and avoid a ban. These type of hardware bans are only administered when the player tries to tamper with the PunkBuster software though, not the game software.

This disabling of the accounts, meaning that the customer loses the right to play, can thus be done by private server administrators in FPS-games – sort of a vigilante effort. Those servers are owned by private people, not the company who developed or published the game, and they can ban or kick anyone they want without obligations. The developers and publishers however, can not ban anyone from playing without good reasons. (E.g. from their MMORPG server or from Battle.Net, after all, the customer have paid for the service.) Therefore they often refer to violations of the EULA when they suspend accounts, which bring me to the next topic.

[165] http://www.punksbusted.com Noteworthy is that PunkBuster comes with it's own EULA.

5.5 Validity of anti-cheating clauses

The EULA is the main legal tool that game developers and publishers rely on when suspending accounts and banning players who have used some sort of cheat in their games. The basic rule is that the customer have paid for a product which he can not use the intended way if he is banned (the multiplayer online part for FPS and RTS-games, and no play at all if it is an MMORPG). The purchase of the product has created a set of obligations between seller and buyer, where the primary obligation of the seller is to provide the product and the primary obligation of the buyer is to pay. Should this relationship be upset, the buyer not able to use the product he has paid for, the seller has broken his side of the agreement – to deliver. So as not to run afoul of consumer protection (such as a sales act) laws the seller needs some kind of justification for banning the buyer, hence the EULA and its anti-cheat clauses. A contract violation gives the seller the legal right to take action, like revoke the license agreement because the player broke it.

To date, at least to my knowledge, no cheater has been sued in a court. The reason for this is that litigation costs money. Contract law (or civil law) is not designed to punish people; rather it is suppose to put the aggrieved party in the same position as he was before the breach of contract. To this end, the aggrieved party must be able to show that he has suffered damages.[166] There is no question that cheating results in damages, like lower brand value of the game that may result in lower sales. The difficulty lies in proving it in court – e.g. because X (the defendant) cheated Z players will not buy the plaintiffs expansion pack resulting in Y loss of sales for the plaintiff, a statement next to impossible to prove. Therefore the companies stop at the practical measures, prohibiting the behaviour and banning accounts themselves, or contracting PunkBuster to provide some cheat protection.

As I have already discussed above the right for two parties to enter any agreement they wish may be subsequently limited by a court, particularly in a B2C transaction with unilateral terms not subject to negotiation – like a EULA in a click-wrap. To that end, I will analyze some anti-cheating provisions in order to find weaknesses in them that might be exploited.

[166] "Garthilk." http://vanguard.okratas.com/index.php?module=subjects&func=viewpage&pageid=28

Epic Games; Unreal Tournament 2004[167]

5. CHEATING. Nobody likes a cheater. It's a disgraceful way to earn a win and really is an insult to those players who earn their wins in on-line games the old-fashioned way—WITH TALENT. We're pretty hard on cheating in on-line games using the Software because it sullies the overall gaming experience and is JUST PLAIN LAME. With that in mind if you are caught cheating in an on-line game using the Software we will immediately and permanently ban your CD Key. At that point this License Agreement is automatically terminated and you must immediately delete this software from your PC. Failure to comply with this last bit (deleting the software) may bring on the wrath of the lawyers. Trust us…you don't want that.

Although commendably free from legalese with clear sanctions – ban of CD-key and revocation of the license agreement, and otherwise fairly non-ambiguous sentences I yet see a problem. What is cheating? As I wrote in Chapter 2.4.4, cheating is hardly a uniform term in online multiplayer gaming – can a player be banned in UT2004 for exploiting a bug? If so, every bug or only the "serious" bugs? How much scripting is allowed? The grey area between outright hacks and a clean game is with this clause quite large, and should a case reach the court it may be difficult to determine whether a player have violated the clause. It should be added that a common principle in contract law is *"in dubio contra stipulatorem"*, which means that unclear provisions is interpreted to the disadvantage of the one who wrote them.

In contrast, the MMORPG World of Warcraft and its developer Blizzard takes a much more detailed approach to the issue of cheating;

Blizzard Entertainment; World of WarCraft[168]

2 C. You may not modify World of Warcraft to change game play, including, but not limited to, the creation of cheats and/or hacks, nor may you use any third-party software which is running at the same time as World of Warcraft that accesses files which are part of World of Warcraft, for any reason whatsoever. Additionally, you may not utilize any "packet sniffing" software[169], regardless of

[167] UT2004 is a popular futuristic FPS game. The entire EULA can be found here: http://www.epicgames.com/ut2k4_eula.html

[168] Note that this is from the Terms of Use, not the EULA. The EULA refers to the Terms of Use.
EULA: http://www.worldofwarcraft.com/legal/eula.html
Terms of Use: http://www.worldofwarcraft.com/legal/termsofuse.shtml
The US case "DeJohn v. The .TV Corporation International et al., 245 F.Supp.2d 913 (C.D. Ill. 2003)" stated that a hyperlink in the click-wrap gave the licensee ample opportunity to follow the link to the terms. One can surmise that the same principle is valid for a EULA referring to Terms of Use, although it would not hurt to have the Terms of Use link more visible. To play it safe, anti-cheating clauses should probably be included in the EULA.

[169] Packet sniffers are used by cheat-creators to reverse engineer the software in order to figure out which data streams between client and server to manipulate and enable cheating.

the operating system utilized by such software and regardless of whether or not such tools are running on the same computer as the World of Warcraft software or any computer connected to the World of Warcraft software or its network, or otherwise monitor World of Warcraft's network connection while you or anyone else is playing World of Warcraft.
2 F. You may not modify any files which Blizzard Entertainment does not specifically authorize you to modify.

...you may not:
3 B viii) Cheat during game play, including but not limited to modification of the game program files.
3 B ix) Participate in any action that, in the opinion of Blizzard Entertainment results in an authorized user of World of Warcraft being "scammed " or 'defrauded' out of gold, weapons, armor, or any other items that he/she has earned through authorized game play in World of Warcraft.
3 C i) You may not use or "exploit" errors in design, features which have not been documented, and/or "program bugs" to gain access that is otherwise not available, or to obtain a competitive advantage over other players.
3 C (iii) You may not use any tools which hack or alter the World of Warcraft client or server software.
3 C (iv) You may not use software products which "packet sniff" or provide scripting and/or macroing to obtain information from World of Warcraft to gain a competitive advantage over other players.
3 C (v) You may not do anything that Blizzard Entertainment considers contrary to the "essence" of World of Warcraft.

12 D. In order to assist Blizzard Entertainment to police users who may use "hacks," or "cheats" to gain an advantage over other players, you acknowledge that Blizzard Entertainment shall have the right to obtain certain information from your computer and its component parts, including your computer's random access memory, video card, central processing unit, etc. This information will only be used for the purpose of identifying "cheaters," and for no other reason.

The contrast to Epic Games anti-cheat clause could not be greater. It gives Blizzard a carte blanche in dealing with cheaters, as every conceivable way of cheating is covered and forbidden. Even tweaking done outside the in-game menus is prohibited (section 2F)[170], and a general clause forbidding anything Blizzard finds contrary “to the “Essence” of World of Warcraft” (3Cv). I see no legal reason as to why these sorts of contracts should fail to be held up in court. It is detailed, with little room for ambiguity, it tells the player exactly what he can and can not do in order to comply with the license agreement. Furthermore, I do not think it can be seen as unreasonable in the light of that all a player have to do, in order to be absolutely sure he complies with the provisions, is to play the

[170] I interpret the clause as ”specifically authorized” means files that can be manipulated via the game interface, whereas other types of manipulation (like altering code manually or with a program) is forbidden.

game "as-is". What conceivably could turn out to be a problem with these kinds of contracts is the issue of tweaking. Minor changes in order to achieve optimum performance are as such forbidden by Blizzard if the player access files outside the in-game menus, which in my opinion is unreasonable. The problem is easily rectified though; Blizzard could for example provide a tweak-guide with approved modifications. Even more likely is that they will refrain from invoking the sanctions for modifications that are not meant to gain unfair advantages in the spirit of cheating. Another potential problem to be recognized is the information obtaining clause (12 D). Similar to PunkBuster, Blizzard agrees with the player that they can access his computer at will and extract information. Eventually, integrity issues may arise. How far can gaming companies go to combat cheats in this way?[171] Furthermore, contractual provisions may clash with mandatory laws regarding the right to privacy and the handling of gathered data.

The biggest flaw regarding combating cheats contractually is obviously that persons not bound by the contract are not subject to its rules. License agreements can be broken at any time the end user wishes; all he has to do is remove the game from the computer and get rid of its physical media.

Epic Games UT 2004 EULA

6. Termination. This license is effective until one of us terminate it. You may terminate this license at any time by destroying the Software and related documentation. In the unlikely event that you are naughty and fail to comply with any provision of this license, this license will terminate immediately without notice from us. Upon termination, you must destroy the Software and related documentation. Please don't wait for us to come after you; it would not be pleasant for either of us. If we do have to come after you, we're going to expect you to pay us for our troubles, including the cost of our lawyers.

Blizzard Entertainment World of Warcraft EULA

5. Termination. This License Agreement is effective until terminated. You may terminate the License Agreement at any time by (i) destroying the Game; (ii) removing the Game Client from your hard drive; and (iii) notifying Licensor of your intention to terminate this License Agreement.

He can then not play the game of course, but the EULA will not stop him from subsequently creating and spreading cheats to the game. It is therefore important to be able to rely on other means of combating cheats, such as copyright and trademark laws.

[171] This is however, as I've already said before, the subject of an entire paper in it self.

Consider the difficulties, in a court situation, of actually proving the defendant is or was bound by the license agreement. Also note that many EULAs (as the Epic Games license agreement) does not even forbid the creation of cheats, only the use of them.

Chapter 6: Cheating – the Crime?

Civil law, which I have written about this far, like a contract violation or a copyright infringement is in the eyes of the law a matter concerning only the involved parties. If one party wishes to resolve the matter in court he has to handle it himself, filing a lawsuit, drafting claims etc, and bear the costs thereof himself.[172] The opposite of that is criminal law (or penal law) which regulates governmental sanctions, imprisonment and fines, in the interest of social order. Certain actions are dubbed crimes by the law, and the court proceedings are handled by the state in the form of prosecutors. The state bears the costs for the trial. The questions are; 1) can the creation and spreading of hacks be a crime? 2) Can cheating in multiplayer online games be a crime?

The answer to the first question is yes; depending on the circumstances the creation of hacks can be a crime punishable by law. Intellectual Property violations as a crime is handled in article 61 of TRIPs, which states;

Article 61 (TRIPs)[173]
Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

Thus, *if* the creation of hacks is a copyright violation and done wilfully on a commercial scale (like systematically selling hacks) there is a chance that it might be seen as a crime. This depending on the national legislation in question, and the same goes for prospective trademark infringements in the course of spreading cheats.

[172] It should be noted that the loser of a civil case in some legal systems must pay for the winner's costs as well, nevertheless it may not be easy to predict the outcome of a trial and suing someone always means that you are taking a financial risk.
[173] http://www.wto.org/english/docs_e/legal_e/27-trips.pdf

The answer to the second question can also be yes. In Chapter 3.2 I explained the difference between client-side based games and peer-to-peer based games, and the basics of the communication between server and client. There is a vital distinction between the client and the server, a hack targeting a server or indeed any computer but one's own (whether for cheating purposes or not) can be a crime punishable by law – a so called cyber crime. Here is a gaming related example;

"Another case reported that a person lost his item bought at around US$220 and called the police, and the investigation showed that the theft was by the person who sold the item - he hacked the game site, and stole the item back after selling it…"[174]

Legally, hacking someone's character account via the game site to obtain items in an MMORPG is a cyber crime, but it is very uncertain that it is a theft in the eyes of the law.

The field of cyber crime knows no national boundaries, and pressure for harmonization is ever increasing. The situation that a malicious cracker[175] can sit in a country which does not punish the unauthorized access to a computer system and thus get away with it is clearly unacceptable (it also raises complicated questions of jurisdiction – where did the actual crime take place?). The Council of Europe[176] (CoE) is an association of European countries distinct from the European Union (although all EU member states are members of the CoE, it also has members not part of the EU). It has produced a Convention on Cybercrime, currently signed by 41 countries (ratified by nine)[177] including non-European countries USA, Canada, South Africa and Japan. Article 2 states[178]:

Article 2 – Illegal access *(Council of Europe Convention on Cybercrime, No. 185)*
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

174 Yan et. al. http://puck.emeraldinsight.com/vl=727129/cl=128/fm=html/nw=1/rpsv/cw/mcb/02640473/v20n2/s6/p125
175 Mainstream media uses the term "hacker" for computer criminals, and cheats in online games are called hacks. Hacker, however, also have a positive denomination as a person who is good at, and enjoys programming. See the Jargon File http://www.catb.org/~esr/jargon/html/H/hacker.html, which dubs the computer criminal "cracker".
176 http://www.coe.int
177 List of signatories found here: http://conventions.coe.int/treaty/EN/cadreprojets.htm
178 Full text of the Convention found here: http://conventions.coe.int/treaty/EN/cadreprojets.htm

The article is very generally written, and leaves the exact implementation to the individual member states. Also criminalized are the aiding, attempting and abetting of illegal access, according to Article 11.

This piece of legislation means that the signatory parties must criminalize unauthorized access to computer systems, which in turn means that cheats which requires access to someone else's computer or server is a criminal offence. Examples of such crimes would be to hack the servers of an MMORPG to gain access to objects, although it should be said that the vast majority of cheats are done client-side – especially in RTS and FPS-games. Whether a country have signed and ratified international treatises regarding cyber crime is in a way irrelevant, an educated guess is that within the western civilization and its sphere of influence a majority of the countries has some sort of legislation regarding illegal access to computer systems along the lines of the CoE Article 2, or they will have shortly. The risks of computer cracking are too high for it to be left alone, the stakes having the potential of being in the order of millions of Euros.

In Chapter 2.2 I mentioned the growth of Internet based games of chance (this subject is strictly speaking beyond the scope of this essay, nevertheless, I can say a few words about it), such as poker, and stated that traditional cheating, as we see in the genres of FPS, RTS games and MMORPG's is rare. The reason for this is that nearly all information that a cheater needs to cheat is placed on the server – thus the conclusion is that every attempt to crack the server, e.g. in order to see the opponent's cards or some such, is a cyber crime.

Chapter 7: Looking Towards the future of Online Gaming

- A comparison between sports and cybersports.

There are striking similarities between cheating in online gaming and cheating (the use of illegal substances) in sports[179].

- The use of illegal substances to enhance performance and the use of cheats must both take place covertly to be effective.
- It is impossible to tell if someone is cheating or using illegal substances by just observing them (over the Internet for cyber sports – actually standing behind someone's screen will reveal any cheats). Although strong suspicions may arise, it is impossible to prove anything conclusive by merely observing someone play well or run 100 meters really fast.
- Doping and cheating in online games is often illegal, i.e. possession and use of some drugs used to enhance performance is subject to criminal law outside the sports context. Cheats in the form of hacks may violate civil law (infringing copyrights and trademarks and breaking contracts) and criminal law.
- Athletes and cyberathletes caught cheating are subject to a serious decline in reputation. Athletes stand to lose much more of course, in pure monetary terms and worldwide attention in the form of loosing sponsorships and bad press (the athlete's trademark value plunges). Cyberathletes are equally shunned, loosing all the good reputation they have built up in their nickname, and frequently the clan they belong to suffer as well (any serious clan or guild[180] will kick a caught cheater and denounce him). Nevertheless, cyberathletes can disappear and resurface with a new nickname, which athletes naturally are unable to do.
- Counteractions include invasive methods, e.g. making athletes take unannounced tests in between competitions and scanning the cyber athlete's computer.

[179] When I write sports, I basically mean every conceivable sport performed in the real world, i.e. not on a computer, specifically in which it is possible to enhance the performance by using drugs. Cyber sports refer to organized competing in computer and video games – i..e ladder play.
[180] Guild is a MMORPG (or MMOG) phenomenon, the counterpart of clans in RTS and FPS-games. A guild is a congregation of players, who cooperate and socialize, solving quests together and generally helping each other out. Depending on game type, rivalling guilds and other types of factions can go to war against each other.

- Avoiding tests is tantamount to guilt for both athletes and cyberathletes (e.g. tampering with the anti-cheat software).

Consider one of the most used excuses for athletes caught using illegal substances (doping); "it wasn't me, my coach/agent/an unknown person with sinister intentions spiked my water with the drug". While perhaps true in a few cases, it would nonetheless be impossible to find anyone guilty of doping if every athlete could get away with that excuse. Now, take any gaming-ladder organization and follow the news, sooner rather than later someone will pop up having cheats installed on his computer, and the players excuse is often "it wasn't me, my friend/brother/an unknown person with sinister intentions invaded my computer and installed the cheats" or "I was just testing". The evident ease of which the accused person can cast doubt over cheating allegations with excuses such as this has lead both the sports law and the cybersports anti-cheating efforts to adopt a strict zero tolerance policy. Anyone found having cheats on their computer or drugs in their system are guilty of cheating if they can not prove otherwise (a shifted burden of proof)[181]. Naturally, anyone caught red handed, with the needle in their room or a valid screen shot of the cheat is busted. Similar to sports, cheating in cyber sports have grown more and more sophisticated. Designer drugs that can not be traced in samples corresponds with cheats that can not be traced by scanning the computer – unless the person searching for the cheat or drug knows what to look for.[182] I.e. the drug is known and traces of it can be analyzed, or the cheat is known by the program scanning for it.

The point is that the companies involved in the gaming industry and the various non-profit anti-cheating organizations may have a lot to learn from how the sports have handled the issue of cheating. If we presume that cybersports will continue to grow, we must suppose also that the problem of cheating will grow. As I have already mentioned several times, the professional cybersport, as of today, does not have any significant problems with cheating since their competitions are hosted at LANs. Nevertheless, a very small percentage of the gaming community can afford to travel (usually via sponsorships) to LANs at a regular basis to compete. The fact that you can stay in your home and compete is also one of the reasons why cybersports has grown so much the last couple of

[181] Jones, P 30.
[182] A new form of doping have recently been predicted, gene doping. It alters certain genes in order to enhance performance, and it may be impossible to detect. Although it is not possible today, there is a growing concern over this form of doping. See e.g. http://www.acfnewsource.org/science/gene_doping.html

years. If that growth is to continue, it is my belief that the cheating problem must be dealt with at a much more conclusive level. The involvement of money and other tangible prizes for online tournaments have become more and more frequent as ladders and companies strive to distinguish themselves on the market, thus the incentives for cheating have only grown bigger.

Sports have attacked the issue of cheating legally by building up organizations whose members are required to follow the rules of that organization. Organizations on the national level have in turn joined international organizations, for example we have a Swedish football[183] association which is a member of the Union of European Football Associations (UEFA), which in turn is a member of the world organization Fédération Internationale de Football Association (FIFA). FIFA have in turn signed the World Anti-Doping Agency's (WADA) Code, together with many other international sports associations, Olympic committees, national anti-doping agencies, 163 governments and so on[184]. This massive membership at the various levels of organizations allows them to create, in essence, their own laws.[185] If an athlete breaks the rules of organization by cheating, e.g. breaking the WADA Code, he will face a disqualification effectively banning him from continued competition within his sport worldwide. Since the stakes are high, a professional athlete lives upon his ability to compete, the rules are subject to heated discussions, and cases might even end up in civil courts. An independent arbitration court for sports have been created, the Court of Arbitration for Sports (CAS)[186], which on the request of both parties judge cases with binding decisions – just like any other arbitration court but specializing in sports related issues.

A similar structure has been emerging for cybersports, albeit without the same formality. Ladder organizations and MMORPG's set up rules that the players must adhere to – failure to do so may result in a ban from the ladder or the account. The ban, however, is only for that specific ladder or game[187] - and each ladder or organization has its own (informal) rules or system for appeals (mainly consisting of trying to prove innocence).

[183] Or soccer, as the Americans calls it. Why do they call the sport football anyway, they all grab the ball with their hands.
[184] http://www.wada-ama.org/en/dynamic.ch2?pageCategory_id=161
[185] The field of sports law is a legal discipline of its own, the space is not sufficient to describe it here.
[186] http://www.tas-cas.org/default.htm
[187] The only exception I am aware of is tampering with PunkBuster software, which will lead to a ban from all PunkBuster supported games.

7.1 A cybersport organization?

The task of eliminating cheats in online multiplayer games can be seen as being of Sisyphean dimensions. Nevertheless, most efforts to date have consisted of a software battle, in which the anti-cheating efforts have focused on pitting their anti-cheat software against the cheaters, who in turn have tried their best to outsmart the software with new programs. The focus in this paper thus far has largely been to analyze the legal situation, with the evaluation of their effectiveness to come in Chapter 8. Another method to attack the issue of cheating in games could be to model an organization after how the sports world has handled the issues of doping. Such an organization could easily bind all its members to its rules by way of electronic contracts, click-wraps.

Such an organization would, to be effective, have to include all major ladders, leagues and cyber sports organizations, the major publishers and developers and anti-cheating organizations. Could these actors unite and cooperate in the cheating issue, like the sports world has done in WADA, the struggle to stop cheating would reach new heights. Some way to include the cybersports principal members as well, the gamers, should also be found. The benefits are particularly;

Eliminating anonymity
One of the problems, as I see it, with cheating today is the lack of ramifications for caught cheaters, and the "moral vacuum" online gaming anonymity enables[188]. At the best, the cheater is caught by someone with the ability to ban his CD-key from further play (e.g. by a PunkBuster server who streams to PunksBusted's MBL, or an MMORPG who can ban accounts) and his nickname is recognized as a cheater and shunned by the community. Nevertheless, any cheater can disappear and reappear under a new identity, most often by simply acquiring a new CD-key or creating a new account. If this anonymity would disappear, coupled with serious "punishments" for cheating, a significant decrease of cheating would be the effect. Such punishment could, like in the sports world, consist of a two year ban from all online gaming competition under the umbrella of the organization. If players could be conclusively identified no matter what online identity they assume there would be no way of disappearing after being caught cheating, and then resurfing with a new identity. The ban would also be valid for all games under the organization, in all ladders and all MMORPG's. Identification could

[188] Pritchard, http://www.gamasutra.com/features/20000724/pritchard_pfv.htm

consist of hardware GUID's[189], with the player obligated to report new parts he acquires. Being caught would therefore entail significant costs for the players; they will be unable to play games competitively online (or at all) unless they acquire what amounts to a new computer. The cost of cheating would thus increase significantly.

Legitimacy

An explosive growth of online gaming in various forms and shapes has taken place of the last few years, and it will only continue to grow as connectivity and computer availability increases. More and more money is being invested to create and sustain games, and the amount of time invested by the players grows as well. You can actually make a living out of acquiring virtual objects in MMORPG's and selling them on auction sites. With the involvement of money, the question of cheating will become more and more serious – an allegation and a subsequent ban for cheating could actually be devastating for an individual. The time invested by the player, who has built up a reputation in the gaming community, is in some cases quite significant. Being caught cheating destroys all that effort and time. If the cyber sports are to grow it is important to install a system of legal security. There is a lack of transparency and predictability about the anti-cheat system as it exists today. With clear, unambiguous rules and regulations, with a governing body that openly presents its rulings, a new organization could bring transparency and predictability to the world of cyber sports in unprecedented ways.

Economics

Perhaps one of the reasons as to why cheat-creators have not been sued in courts is the question of money. Lawsuits are expensive, and other means of stopping cheats are more cost effective. A joint organization, however, would be funded by its members and have a budget of its own. Cost effectiveness could be reached by having the organization carefully select pilot-cases on behalf of the entire industry in order to create a case-law on the subject in the most important jurisdictions. Cooperation would mean the costs for going to court will be significantly lower on any one part, and valuable precedents will be set to the benefit of all the actors in the online gaming business.

[189] Globally Unique Identifier, see http://en.wikipedia.org/wiki/GUID for more information. Hardware GUIDs are a sequence of numbers computed based on the hardware, i.e. each graphic card, motherboard etc. is assigned a unique hardware GUID. PunkBuster already employes hardware GUID bans, as punishment for tampering with their software.

Chapter 8: Conclusions

It is a fact that cheating in online multiplayer games is a problem that needs to be dealt with. The reasons are fairly simple; a game with copious amounts of cheating will lose sales and customers. Furthermore, it is reasonable to assume that not only the game brand will lose value; a cheat-infested game will have a harder time selling expansion packs and sequels besides selling copies of the game itself. At the worst, the companies behind the game will lose overall sales as their brands become associated with games in which cheating is ubiquitous. Since most players abhor cheating in online multiplayer games and would love to see the problem eliminated, taking a hard stance on cheating in games has largely positive effects.[190] The company that can show that they take the problem of cheating seriously in their games will gain goodwill and might raise sales just because of that. Although promising an absolute cheat-free game is utopian today, the company that comes near that vision will raise their brand value and thus attract gamers who desire a cheat free gaming environment. As a general rule a company should avoid attacking its own customers with legal remedies on any kind of regular basis, as such behavior only serves to alienate the customers and incur badwill towards the company. The problem of cheating is an exception. The clean players, i.e. the large majority of the customer base, detest the cheaters and would love to see them "brought to justice".

Generally speaking, the computer gaming segment can be divided into two distinct categories; hardcore and casual gamers[191] (also called fungamers). This concept can be carried over to the multiplayer part of the gaming scene; the hardcore gamers are "in the loop", plays often, many of them are clan-members and play competitively on ladders. By contrast, the casual player merely pops in every now and then for a few rounds of fungames. Since the casual players are the vast majority[192], the gaming companies naturally desires to attract a bigger crowd of casual players to their game. However, the casual gamer have not invested as much time and effort as the hardcore gamer into any one game, and is thus much more likely to simply walk away from a brand. If the casual players experience cheats, or what they label cheats, they will leave for another game.

[190] This can, however, produce a backlash, as crackers might perceive a company's stance as a challenge, and thus intensify their efforts in creating cheats and releasing them to the game. PunkBuster frequently faces this problem, as some crackers try to crack their software just for the fun of it.
[191] Kofler et. al. P 34. http://ep2010.salzburgresearch.at/knowledge_base/kpmg_2002.pdf
[192] Ibid, P 35.

So, what legal measures can be taken to eliminate, or at least minimize, cheating in online multiplayer games?

- The creation of cheats

The line of reasoning presented in Chapter 3 can be used to argue that the creation of cheats is very likely to violate copyright laws both in Europe and in the US (although the situation is murkier in the US), and thus that hacks constitutes copyright infringement. However, searching out and suing every gamer who creates hacks is not economically viable; the costs for such measurements are perhaps not worth the gain. The first few cases could be justified, to get a ruling on the issue and spread awareness in order to deter other cheat-creators, but other than that; attacking each individual would simply expend too much resources. Other venues must therefore be explored.

- The spreading of cheats

Since most cheaters can not create their own cheats, for a variety of reasons (such as lack of time and skill), targeting the ones who create and spread cheats must be a priority. Using trademark laws to prevent cheat distribution is a very uncertain path. First of all, only those who actually sell cheats are liable to be guilty of trademark infringement and many cheats are freely spread. Secondly, my analysis is that the prospects of winning a trademark suit against those who sell cheats are slim; although the chances increase if it can be proved that the trademark is well known. A better and more cost effective path would be to use the DMCA takedown provisions and the similar rules from Europe under the e-Commerce Directive to target the sites on which the cheats are spread and discussed. If such sites are hunted down and deactivated, most cheaters would not have a place to collect their hacks. So lawsuits should be used sparingly, and against a few of the bigger fishes only, and shutting down websites which spreads infringing material ought to be prioritized.

- The use of cheats

Eliminating the “grey area” (discussed in Chapter 2.4.2) by producing official, clear guidelines about cheating is an effective way of alleviating some of the negative effects from cheating. First of all, the casual gamers will gain knowledge about the issue and can much easier, when confronted with suspicious actions, determine if it is within the allowed area or if they should suspect cheating. In essence – it will level the field of play in the sense that the hardcore gamers won’t have “exclusive” access to advanced tweaks and scripts in the borderland of cheat/non-cheat – as the rules will be clear to all.

Secondly, if the guidelines are clear, it is easier to ban, or use other sanctions against, players who cheat via the contractual provisions. Unclear rules about cheating will only create confusion and resentment. Thirdly, contracts which are clear and unambiguous have a much better chance if being declared valid in court, should a case reach that far (which is more and more likely considering the development and growth of the computer gaming industry). The fourth and final reasons are the issues of transparency and predictability; clear unambiguous contracts serves to make the decisions on what cheating is to be transparent, meaning that all gamers (hardcore and casual) can easily understand and appreciate the rules, as well as predict the outcome of being caught cheating.

- Cheating, the crime

Cheating and its related actions can, under certain circumstances, be a crime punishable by law. In those instances, i.e. massive commercial intellectual property infringements and cyber crime in the form of unauthorized access to servers and computers, the most cost effective and deterring action is to report it to the authorities. Naturally, the more evidence that can be turned over to the prosecutor and the police the better, but otherwise the authorities will conduct the necessary investigations and trials. Therefore all such activities should be reported to the police immediately.

- The Future

The similarities between cheating in sports (doping) and cheating in cybersports leads, in my opinion, to the conclusion that lessons from the sports anti-cheating methods can be used in cyber sports as well. Particularly that of an umbrella organization with a code, such as WADA, consisting of the companies and organizations involved in the business, as well as the gamers themselves (via the use of electronic contracts similar to those already in existence today, online gamers can be bound by the code in order to play online). The benefits would be possibility to eliminate the anonymity that cheaters crave and methods of banning not just for a certain set of servers, a single ladder or game, but for all servers, games and ladders – thereby making the punishment for cheating really deterring.

Chapter 9: Sources

9.1 Table of Articles

Aarseth, Espen. "*Playing Research: Methodological Approaches to Game Analysis.*" March 10, 2004.
http://hypertext.rmit.edu.au/dac/papers/Aarseth.pdf,

Bartle, Richard. "*Hearts, Clubs, Diamonds, Spades: Players Who Suit MUDs.*" 20 July, 1996.
http://www.mud.co.uk/richard/hcds.htm

Carmack, John. *"News post."* December 25, 1999.
http://www.bluesnews.com/cgi-bin/finger.pl?id=1&time=19991226003141.
Carmack John.* *"Forum post."* December 26, 1999 from Slashdot.
http://slashdot.org/article.pl?sid=99/12/26/1255258&mode=thread

Collins, John. "*The benefits of Click-Wrap contracts over Shrink-Wrap Contracts*" November 27, 2003.
http://www.design-ireland.net/index.php?http%3A//www.design-ireland.net/e-commerce/business-12.php

Contreras, Jorge L. and Slade, Kenneth H. *"The Origin of Click-wrap: Software Shrink-wrap Agreements."* March, 2000.
http://www.wilmerhale.com/publications/whPubsDetail.aspx?id=1c693d50-4976-4339-989a-bff98bb48730

Communication to the European Parliament, the Council, the Economic and Social Committee and the committee of the Regions. *"Illegal and harmful content on the Internet."* November 5, 1999.
http://europa.eu.int/ISPO/legal/en/internet/communic.html.

Darden, Laura and Thorpe, Charles. *"Forming Contracts Over the Internet: Click-wrap and Browse-wrap Agreements."* Summer 2003, Georgia State University, College of Law, Law and the Internet.
http://gsulaw.gsu.edu/lawand/papers/su03/darden_thorpe/#II

Dibbel, Julian. *"Black Snow Interactive and the World's First Virtual Sweat Shop."* January 2003.
http://www.juliandibbell.com/texts/blacksnow.html

Egenfeldt-Nielsen, Simon and Heide Smith, Jonas. *"Online gaming habits"* April 7, 2002.
http://www.game-research.com/art_online_gaming.asp.

"Garthilk". *"Interview with Don Shelkey"* September 7, 2004.
http://vanguard.okratas.com/index.php?module=subjects&func=viewpage&pageid=28

Gaudiosi, John. *"Games, Movies, Tie the Knot"* 10 December, 2003.
http://www.wired.com/news/games/0,2101,61358,00.html

Grossman, Mark et. al. *"Click-Wrap Agreements - Enforceable Contracts or Wasted Words?"* 2004.
http://www.becker-poliakoff.com/publications/article_archive/click_wrap.htm

Hargreaves, Shawn. *"The Easy Route to Console Online."* 2004, Game Developers Conference Presentation.
http://www.talula.demon.co.uk/ConsoleOnline.pdf
Hargreaves, Shawn.* *"Playing the Open Source Game."* July 1999.
http://www.talula.demon.co.uk/games.html

Karjala, Dennis S. *"Copyright Protection of Computer Software, Reverse Engineering, and Professor Miller"* Spring 1994, University Dayton Law Review.
http://homepages.law.asu.edu/~dkarjala/Articles/DaytonLRevSpring1994.html.

Kofler, Peter and Fonnesbech, Christian. *"The Interactive Culture Industry"* July 4, 2002, For the Danish Ministry of Culture.
http://ep2010.salzburgresearch.at/knowledge_base/kpmg_2002.pdf

Kuo, Andy. *"On Cheating." March 22, 2001.*
http://shl.stanford.edu/Game_archive/StudentPapers/BySubject/A-I/C/Cheating/Kuo_Andy.pdf

Lloyd, Ian. *"Legal Issues of Shrink Wrap Licenses".* 1996.
http://europa.eu.int/ISPO/legal/en/tourtabl/lloyd.html

McCarthy, Thomas J. *"Dilution of a Trademark: European and United States Law Compared."* 2004. Based on a contribution made to the collection of essays entitled Intellectual Property in the New Millennium. (Cambridge Univ. Press), Vaver & Bently (eds.), which is a Festschrift in honor of Professor William Cornish of Cambridge University.
http://www.inta.org/downloads/tmr_McCarthy.pdf

Marzouki, Meryem. *"E-commerce directive transposition raises serious privacy and free speech concerns in France."* February 02, 2003.
http://www.edri.org/edrigram/number2/france

Moses, Asher. *"Cheating: Multiplayer Gaming's Achilles' heel?"* May 17, 2003.
http://www6.tomshardware.com/game/20030517/index.html

Pawlo, Mikael. *" Shrinkwrap- och clickwrap-avtal i svensk och internationell rätt"* Nordiskt Immateriallt Rättskydd, 1/1999 140.

Pritchard, Matt. *"How to Hurt the Hackers: The Scoop on Internet Cheating and How You can Combat It."* July 24, 2000.
http://www.gamasutra.com/features/20000724/pritchard_pfv.htm

Ramberg, Christina (formerly Hultmark-Ramberg). *"The E-Commerce Directive and Formation of Contract in a Comparative Perspective."* 2001, Global Jurist Advances, Volume 1, Issue 2, Article 3.

Raymond, Eric S. *"The Case of the Quake Cheats"* 27 December, 1999.
http://www.catb.org/~esr/writings/quake-cheats.html

Reinius, Fredrik "NewmaN". *"Exklusiv förhandstitt på Battlefield 2: Intervju med Lars Gustavsson."* February 20, 2005.
http://www.bfcentral.se/?s=article_show&id=525&pn=9

Roberston, Struan J.A. *"The Validity of Shrink-Wrap Licences in Scots Law Beta Computers (Europe) Ltd v. Adobe Systems (Europe) Ltd"* June 30, 1998.
http://elj.warwick.ac.uk/jilt/cases/98_2rob/dwnloadf.htm

Rogers, Douglas L. *"The future of Software Bundling after United States v. Microsoft."* December 2001. Reprinted from Intellectual Property & Technology Law Journal at:
http://www.vssp.com/CM/Articles/articles794.asp.

Rolston, Bruce. *"The secret life of Gooseman."* December 30, 2000.
http://www.avault.com/articles/getarticle.asp?name=gooseman&page=1
Rolston, Bruce.* *"Look before you click, Part I, Do you really know what's in your EULA?"* December 8, 2000.
http://www.avault.com/articles/getarticle.asp?name=eulapt1&page=1

Sawyer, Ben. *"The Next Ages of Game Development"* September 30, 2002.
http://www.avault.com/developer/getarticle.asp?name=bsawyer1&page=9

Shim, Richard. *"Doom 3 may 'Doom' users' current systems."* August 3, 2004.
http://news.com.com/2100-1043_3-5295390.html

"Simoniker." *"Blizzard Removes 400,000 More Battle.Net Accounts."* October 01, 2003.
http://games.slashdot.org/article.pl?sid=03/10/01/0534202&tid=206&tid=210&tid=10

Stanford Center for Internet &Society (Topic maintained by). *"FAQ Question: What rights are protected by copyright law."* September 1, 2004.
http://www.chillingeffects.org/piracy/notice.cgi?NoticeID=1408#FAQID12053

Wardell, Brad. *"PC Gaming as an industry; Part III; Ideas on what's coming next"* April 9, 2001.
http://www.avault.com/developer/getarticle.asp?name=bwardell3&page=1
Wardell, Brad.* *"PC Gaming as an industry; Part IV; Destroying Myths."* May 7, 2001.
http://www.avault.com/developer/getarticle.asp?name=bwardell4&page=3

Wayner, Peter. *"Do Cheaters ever prosper? Just ask them."* March 27, 2003. New York Times.
http://tech2.nytimes.com/mem/technology/techreview.html?res=9B0DE6DC1E30F934A15750C0A9659C8B63

Yan, Jianxin Jeff and Choi, Hyun-Jin. *"Security issues in online games"* 2002. The Electronic Library Volume 20 Number 2 2002 pp. 125-133.
http://ariel.emeraldinsight.com/vl=2848761/cl=20/fm=html/nw=1/rpsv/cw/mcb/02640473/v20n2/s6/p125

9.2 Table of Books

Anawalt, Howard C and Powers Enayati, Elizabeth. *"IP Strategy – Complete Planning, Access and Protection"*, 2000. West Group.

Cornish, William and Llewelyn, David. *"Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights."* 5th Edition, 2003. Sweet & Maxwell.

DiMatteo, Larry A. *"The Law of International Contracting."* 2000, Kluwer Law International.

Gervais, Daniel. *"The TRIPs Agreement – Drafting History and Analysis."* 1998, Sweet & Maxwell.

Jones, Michael E. *"Sports Law."* 1999, Prentice Hall.

Koktvedgaard, Mogens and Levin, Marianne. *"Lärobok i Immaterialrätt."* 8th Edition, 2004. Norstedts Juridik.

Stamatoudi, Irini A. "*Copyright and Multimedia Works – A comparative Analysis."* 2002, University Press Cambridge.

WIPO (Edited by). "*Introduction to Intellectual Property – Theory and Practice."* 1997, Kluwer Law International.

9.3 Table of Cases

9.3.1 US Cases

American Geophysical v. Texaco, Inc., 37 F.3d 881 (2d Cir. 1994).

Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 584 (1994).

Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. App. Div. 1999).

Comb v. PayPal, Inc., 218 F.Supp.2d 1165 (N.D.Cal. 2002).

DeJohn v. The .TV Corporation International et al., 245 F.Supp.2d 913 (C.D. Ill. 2003)

Forrest v. Verizon Communications, Inc., 805 A.2d 1007 (D.C. 2002).

Hill v. Gateway 2000, Inc. 105 F.3d 1147 (7th Cir. 1997).

Lewis Galoob Toys, Inc. v. Nintendo of Am., Inc., 964 F.2d 965 (9th Cir. 1992), *cert. denied*, 507 U.S. 985 (1993).
http://cyber.law.harvard.edu/openlaw/DVD/cases/Galoob_v_Nintendo.html

Midway Mfg. Co. v. Artic Int'l, Inc., 704 F.2d 1009 (7th Cir.), [**9] cert. denied, 464 U.S. 823 (1983).

Moore v. Microsoft Corp, 293 A.D.2d 587, 741 N.Y.S.2d 91 (N.Y.A.D. 2 Dept. 2002)

Pollstar v. Gigmania Ltd., 170 F.Supp.2d 974, (E.D. Cal. 2000)

ProCD v. Zeidenberg, 86 F.3d 1447, 1450 (7th Cir. 1996)
http://digital-law-online.info/cases/39PQ2D1161.htm

Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238, (S.D.N.Y. 2000)

Specht v. Netscape Communications, 306 F.3d 17 (2d Cir. 2002)

The New Kids on the Block et. al. v. News America Publishing, Inc. et. al. v. Gannett Satellite Information Network, Inc., d/b/a/ USA Today, Inc., Nos. 90-56219, 90-56258. United States Court of Appeals, Ninth Circuit.
http://cyber.law.harvard.edu/metaschool/fisher/integrity/Links/Cases/newkids.html

Ticketmaster Corp. v. Tickets.Com, Inc. 54 U.S.P.Q.2d 1344, 2000 WL 525390, 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000).

Williams Electronics Inc v. Arctic International Inc., 704 F.2d 1009 (7th Cir.), cert. denied, 464 U.S. 823 (1983).

9.3.2 European Cases

Beta Computers (Europe) LTD v Adobe Systems (Europe) LTD Outer House, 1996 SLT 604, 1996 SCLR 587. *(Scotland)*

Hölterhoff v Freiesleben. Judgment of the Court 14 May 2002, Case C-2/00. *(European Court of Justice)* http://oami.eu.int/en/mark/aspects/pdf/JJ000002.pdf

9.4 Table of Laws, Conventions, International Treatises and EC Regulations and Directives

Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs)
http://www.wto.org/english/docs_e/legal_e/27-trips.pdf

Berne Convention for the Protection of Literary and Artistic Works
http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html.

Council of Europe, No. 185 Convention on Cybercrime
http://conventions.coe.int/treaty/EN/cadreprojets.htm (Not a direct link, go to 'treaty office' and acquire it in the left side menu.)

Council Directive of 14 May 1991 on the legal protection of computer programs (91/250/EEC)
http://europa.eu.int/ISPO/legal/en/ipr/software/software.html.

Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark.
http://oami.eu.int/en/mark/aspects/reg/reg4094.htm#0090

Council Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:EN:HTML

Madrid System for the International Registration of Marks.
http://www.wipo.int/madrid/en/legal_texts/

Paris Convention for the Protection of Industrial Property
http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

Swedish Act on Copyright in Literary and Artistic Works (Translated to English)
http://www.wipo.int/clea/docs_new/en/se/se052en.html

Uniform Computer Information Transactions Act (US)
http://www.law.upenn.edu/bll/ulc/ucita/ucita1200.htm

U.S. Copyright Law
http://www.copyright.gov/title17/.

U.S. Trademark Law: Rules of Practice & Federal Statutes.
http://www.uspto.gov/web/offices/tac/tmlaw2.html#_Toc52344284

9.5 Table of Various Resources

Battle.Net, Blizzards ladder site for their RTS-games.
http://www.battle.net/

Blizzard, successful game developer.
http://www.blizzard.com/

Chilling Effects, an organization monitoring the legal climate for Internet activity.
http://chillingeffects.org

Council of Europe
http://www.coe.int

Court of Arbitration for Sport (CAS)
http://www.tas-cas.org/default.htm

Cyberathlete Professional League
http://www.thecpl.com/

eBay, Internet Auction site.
http://www.ebay.com/.

Entertainment Software Association
http://www.theesa.com

Entertainment & Leisure Software Publishers Association
http://www.elspa.com

European Union web-portal.
http://europa.eu.int/

Jargon File, a comprehensive compendium of hacker slang illuminating many aspects of hackish tradition, folklore, and humor.
http://www.catb.org/~esr/jargon/html/

Office for Harmonization in the Internal Market (OAMI)
http://oami.eu.int/en/

Open Source Initiative, an organization dedicated to managing and promoting the Open Source Definition for the good of the community.
http://www.opensource.org/

Player Auctions, auction site specialized in the selling and buying virtual objects and characters in MMOG's.

http://www.playerauctions.com/

PunkBuster, a company that provides anti-cheating software commercially.
http://www.punkbuster.com

PunksBusted, a community dedicated to eradicating cheat by supporting and augmenting PunkBuster.
http://www.punksbusted.com

United Admins, a non-profit organization dedicated to supporting game server administrators.
http://www.unitedadmins.com

Wiktionary, free online dictionary that anyone can edit.
http://en.wiktionary.org/

Wikipedia, free online encyclopaedia that anyone can edit.
http://en.wikipedia.org/wiki/Main_Page

World Anti-Doping Agency (WADA)
http://www.wada-ama.org/en/

World Intellectual Property Organization (WIPO)
http://www.wipo.int/

World Trade Organization (WTO)
http://www.wto.org/